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

Building a Security Test Environment
By: Richard Noël
GIAC GSEC Assignment 1.4b, Option 1

© SANS Institute 2003, Author retains full rights.

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

TABLE OF CONTENTS

ABSTRACT	1
1. Why build a test environment?	1
2. Requirements	2
2.1 Testing requirements	2
2.2 Physical security	2
2.3 Ease of Access	2
2.4 Ease of Restoration	3
2.5 Network Isolation	3
3. VMWare Solutions	3
4. Equipment Used	4
4.1 Computers Used	4
4.2 KVM Switch	4
4.3 Networking Equipment	5
5. Operating Systems Used	5
5.1 Windows Operating Systems	5
5.2 Linux Operating Systems	5
5.3 OpenBSD File Server	6
6. Specific Configuration Requirements	6
6.1 “0” Filled Hard Drives	6
6.2 Network Isolation	6
7. Restoration Procedures	6
7.1 Norton Ghost	7
7.2 G4U Hard Disk Image Cloning for PC	7
8. Possible Test Lab Uses	7
8.1 Employee Training	7
8.2 Forensics Testing	8
8.3 Firewall And Security Appliance Testing	8
8.4 Virus and Exploit Signature Research	8
9. Conclusions	8
Works Cited	10
Test Network Conceptual Diagram	11

© SANS Institute 2003, Author retains full rights.

ABSTRACT

With the increasing number of threats in a networked environment, it has become necessary for many information technology professionals to be informed and aware of how hacker attacks, viruses, Trojans and exploits will affect their systems. An inexpensive test lab with different installed operating systems and countermeasures would be perfect to help research the effects of these security risks, and understand their affect on deployed systems. This paper will discuss the requirements of such a facility, and how a low-cost testing environment was built for this purpose at my company, using older computers and equipment. We will discuss the operating systems and software chosen for the test network, as well as the equipment used, thus demonstrating that anyone with some older equipment lying around could embark on a comparable project with relative ease, while keeping costs at a minimum.

1. WHY BUILD A TEST ENVIRONMENT?

There are several reasons why having a network security-testing environment could prove useful. A test environment could be used to test systems under adverse conditions in a safe manner and without the stress of potential downtime affecting productivity and preventing loss of valuable data. In such an environment, computers can be considered expendable, and the test environment could be used to test how a workstation or server would react when exposed to viruses and exploit attacks. In essence, the goal of a test lab is to provide a controlled set of computers to experiment with security related issues rapidly, and under different software configurations and networking scenarios.

A test lab offers the opportunity to experiment in a way where meaningful data can be gathered and applied to help understand threats under different types of situations. Test computers could be closely observed during an experimental attack in order to gather data on how the systems react, and can be compromised. This data can then be used to find ways to protect against attacks, and develop threat assessments.

IDS' and firewalls could also be tested in such an environment to aid in the development of virus and exploit attack signatures. This data would give IDS analysts and network administrators the ability to more closely monitor and protect their networks.

When we consider the number of new exploits and viruses being released every day, and the number of different operating systems and software packages available to users, the need for a flexible testing environment to conduct research on new threats becomes clear.

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

2. REQUIREMENTS

There are several requirements that have been identified in order to make the lab as useful as possible, and to insure that it meets the intended goals. The lab will require physical security in a climate-controlled environment. Ease of accessing the test stations will also need consideration, as well as the need to easily reconfigure and restore the test computers in the shortest amount of time possible. The test environment's network should not have Internet access, or access to any external network to prevent accidental infection of computers outside the lab.

2.1 TESTING REQUIREMENTS

A security test lab of the type discussed in this paper will be used for testing viruses, exploits, "script kiddy" tools, and other potential security threats in a controlled environment. A lab of this type will be required to provide a clean environment to run experiments to evaluate how these security threats will affect various operating systems, firewalls, IDS' and networks. (1)

2.2 PHYSICAL SECURITY

Due to the nature of the testing, as well as the operating requirements for test environment equipment, the computers and networking components should be located in an area where only authorized administrators can gain access. The test environment will mostly be used for research on viruses, penetration testing, and exploit analysis. For this reason, users should not be given physical access to the machines to assure that there is no possibility of affecting production networks. The test environment components should be located on a separate rack.

It has also been suggested that the lab be wired with a different colour of networking cable that is easily identifiable to prevent accidental connections to the outside world. A colour such as bright red, or bright green, reserved for test lab purposes could be used. (2)

Labels should also be applied to all test lab equipment to identify it as a component of the test environment. The labels should indicate that the systems are restricted for authorized use only.

2.3 EASE OF ACCESS

Despite our physical security requirements, the users of the test environment will need to be able to use the computers in real time. Users will need a way to input data to the machines, and view their output without having actual physical access.

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

2.4 EASE OF RESTORATION

Due to the volatile character of experimentation expected to be conducted in the test environment, it will be necessary to re-install operating systems on the test computers numerous times. Procedures will need to be developed in order to minimise the time and amount of manpower required to complete this task.

2.5 NETWORK ISOLATION

It will be necessary to keep the test environment self-contained at all times in order to prevent accidental damage to either the company's LAN, or to other users of the Internet. Physical security and Air-gapping the network will be a requirement in order to meet these criteria.

3. VMWARE SOLUTIONS

It has been suggested that virtual machines could be used to build a test network. Vmware is a software package that allows a computer to run several operating systems at the same time. Vmware uses a host operating system to launch virtual operating systems that have direct access to the computers hardware. There are several advantages and disadvantages to this approach.

The advantages to using a Vmware lab are that there is no need for multiple computers, as well as the ability to manipulate all the operating systems from one mouse, keyboard and monitor. Vmware can run up to eight virtual machines on a single computer. The way in which Vmware handles images would also aid in quick restoration of a test operating system to a baseline state. (3)

The disadvantage to this approach is the cost of a computer powerful enough to run Vmware. The application is very memory intensive. Vmware can only access system memory below 1 GB. The suggested specifications for a system running five to eight virtual machines is

DUAL CPU 1+ GHz or (1) 2.0+ GHz
1.5 GB RAM
HD (2) 7200 RPM RAID 0 stripe
Drive Space 60+ GB

The cost of such a system would be prohibitive. Vmware also handles networks in a "virtual network" fashion. This would prevent users from testing with different types of network appliances such as IDS sensors that need to be connected on a physical hub and could not be connected to a virtual hub in a Vmware environment. (4)

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

4. EQUIPMENT USED

The computers used in our test environment are older computers that are no longer used in our production environment and serve no useful purpose. We chose to dedicate a separate rack for these computers, to insure they are separate from any production servers. The rack will be located in the server room in order to accommodate physical security and operating environment requirements. The computers will not be physically accessible to those who will be using them; we will use a KVM, which will aggregate the input and output of the computers into a station located remotely, as well as a local administrator's station in the server room where the equipment is located.

4.1 COMPUTERS USED

The test environment will consist of 5 computers. In order to insure the usefulness of the operating system images, all of the computers are identical. This will make restoration easier as one template image can be used on any of the computers. Different driver combinations will not be needed. The fifth machine has more storage capacity in order to store operating system images for deployment.

The fifth machine will run OpenBSD, and will act as a DHCP server, and as a fileserver (via FTP). It is the only machine that will not be considered expendable, and as such will be protected from possible infection from the other computers in the test environment. This machine will be used to store all the operating system images for the other computers, as well as a standard set of tools for testers to use.

4.2 KVM SWITCH

In order to comply with requirements for physical security, the computers for our example test environment will be located in a sever room. In order for users to access the machines, we chose to use a KVM switch. The switch is a Cybex Longview series KVM switch. The system consists of 3 units, the Advocent switch, the Longview transmitter, and the Longview receiver.

The Advocent Switch is mounted on the rack with the computers, and is where the output from the machines will be aggregated. The local terminal, for use by the system administrator locally in the server room, is also connected here. The switch is then connected to the Longview Transmitter. The transmitter sends the signal from the switch to the receiver. This is done via Cat 5 cable. The cable is connected to the receiver, which can be up to 500 feet away. (5)

The remote station is simply a monitor, mouse and keyboard connected to the receiver. From here the operator using the test environment can power cycle the

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

computers, as well as control them from power up thus allowing access to the BIOS.

4.3 NETWORKING EQUIPMENT

For building the network we will be using 2 rack mount 100 megabit hubs. Using hubs will allow the use of software packages that require Ethernet hardware running in promiscuous mode such as sniffers and IDS sensors.

5. OPERATING SYTEMS USED

The operating systems chosen for use on the test network were meant to represent the most common deployed in the real world today. They include both workstation and server operating systems in order to make the lab as flexible as possible.

5.1 WINDOWS OPERATING SYSTEMS

The Microsoft Windows family of operating systems is by far the most widely used in home and office environments today. Images were made of the following Windows versions; Windows 98, 2000 Professional and Workstation, NT 4.0 Server and Workstation. The operating systems were installed unpatched and with no software installed in order to provide a baseline. The only installed services and options are the ones selected by default by the installation process. Service packs will be made available to users on the test lab FTP server. This will allow testing under different patch levels for each of the operating systems.

It is important to note that because of licensing it is important that an image only be loaded on one machine at a time, as the image will have the product key already loaded. If multiple machines running the same operating system are needed, then different images should be made with different product keys to guarantee compliance with End User Licence Agreements.

5.2 LINUX OPERATING SYSTEMS

Computers using Linux are widely used to run servers that are on the Internet. Linux comes in various distributions. We have chosen to make available to users images of Mandrake 9.0, and Red Hat 8.0. As with our Windows images, we will only be doing a default install to provide a good baseline.

These Linux operating systems can be downloaded freely off the Internet and are public domain software. These images can be loaded on multiple computers at once.

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

5.3 OPENBSD FILE SERVER

Our test lab will also include and OpenBSD file server. The file server was built from the computer with the most storage capacity. This machine will not be considered expendable. The machine will host an FTP server that where users can choose the images they'd like to install, as well as software tools and service packs to be applied after the images are loaded.

The OpenBSD file server will not run any service other than FTP and DHCP. DHCP will ease the network configuration necessary for the test environment, as the images can be set to acquire their network configuration from this server.

6. SPECIFIC CONFIGURATION REQUIREMENTS

6.1 "0" FILLED HARD DRIVES

Before the operating systems were installed for creating the images, we used the Linux utility "DD" in order to wipe the hard drive by filling it with zeros. This will prove helpful because it will allow for better compression of the images on the fileserver. Writing the hard drive to zeros will also provide users with clean disks for use in experimenting with forensic utilities where "garbage" on the hard disk could skew results.

In our test lab we used the netBSD utility "dd" to do this. The program is freely available via the standard BSD licence and is included on most BSD boot disks DD is used to copy files. In our case we will instruct the program to write the entire hard drive to zero's in 1 Meg sectors. This will help to speed up the process. From the prompt, the following command was used;

DD if =/dev/zero of=/dev/hda bs=1M

6.2 NETWORK ISOLATION

Our test network will not be connected to the Internet or the company's LAN. This is often known as an Air Gap. We chose to Air Gap our test environment in order to ensure containment of viruses and exploits in the controlled lab. The test environment should not be given the opportunity to infect either innocent users on the Internet, or corporate LAN users where productivity and data loss are possible concerns.

7. RESTORATION PROCEDURES

In order for the test lab to be useable, it is necessary to be able to restore the entire lab to a clean state in a short period of time. In addition, it would be useful to have all the images stored on the same fileserver thus allowing users to customize the configuration of the lab based on the needs of their specific

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

experiment. There are two software packages we investigated for our lab, the first is Norton Ghost Corporate Edition, and the second is G4U.

7.1 NORTON GHOST

Norton Ghost is a well-known application for making hard drive images for deployment over a network. Norton Ghost, however, uses windows File and print sharing in order to load shares over the network. (6) This service is well known to be vulnerable to viruses such as Klez.E, and considering the environment is going to be built to test viruses, and the file server is not to be compromised, it was decided not to use this application in our lab. (7) Norton Ghost is also requires licensing which could become costly depending on the number of client licenses required.

7.2 G4U – HARD DISK IMAGE CLONING FOR PC

G4U was chosen as the candidate for our lab for several reasons. The first of which is that the application is distributed freely under the standard BSD licence. The utility also uses FTP as opposed to Windows NETBIOS. Again, this is important considering the fact that we will be doing virus testing in the lab, and we do not want the file server to be compromised.

G4U images are available for download at http://www.feyrer.de/g4u/#reqs. The website provides raw images which can be written to diskette using a utility such as “rawright” (a link to the utility is provided on the G4U website). The image creates a NetBSD bootable disk with the utility loaded on it. The disk boots the computer to a prompt where the usage for the program is as follows;

To create an image;
uploaddisk <FTP Server IP> <image filename>

To restore an image;
slurpdisk <FTP Server IP> <image filename> (8)

8. POSSIBLE TEST LAB USES

The test lab can be used for a wide variety of things discussed in the introduction of this paper. Some uses include employee training, testing of forensic tools, firewalls, network security appliances, and development of virus and exploit signatures for use in intrusion detection. This section will discuss possible uses for the test lab and software tools that could help in that testing.

8.1 EMPLOYEE TRAINING

The test lab offers an excellent opportunity for security employees to use new tools and evaluate how tools will react in adverse conditions. The test lab can be

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

loaded with both UNIX and Windows based scanning programs, such as the Nessus vulnerability scanner. Testers can also test firewall rules using tools such as Hping. It also gives opportunities to test the functions of tools like Nmap for OS fingerprinting. The lab provides an excellent training tool for employees who will be performing vulnerability scanning, or who will be responsible for intrusion detection.

8.2 FORENSICS TESTING

The test lab can also be used in conjunction with freeware tools such as FIRE. FIRE is a set of tools for use in forensic recovery of data, incident response, and vulnerability testing. The lab offers a clean environment as the hard drives of the computers are reset to zero's when the test lab images are reloaded. This allows employees to become comfortable using these types of tools in a controlled environment protecting vulnerable data on production servers.

8.3 FIREWALL AND SECURITY APPLIANCE TESTING

Firewall and network appliance testing can also be easily accomplished using the test lab. These devices can be easily integrated into the scalable design of the test environment. The devices can then be tested with different tools to evaluate the usefulness and effectiveness of firewall rules and new security appliances entering the market by subjecting them to customized attacks based on a user's specific threat vector.

8.4 VIRUS AND EXPLOIT SIGNATURE RESEARCH

New viruses and exploits are being released on the Internet every day. In order to be able to protect systems against such threats, we first need to be able to detect them. With sniffers and other passive sensing tools installed on the test network, activity from new threats can be analysed by looking at the type of traffic being generated. This traffic analysis can be used to develop signatures for deployed IDS systems in order to detect intrusions and prevent the propagation of new threats. The lab also allows for research and broader understanding of existing threats [(9)]

9. CONCLUSIONS

The usefulness of a test lab is certainly clear. The flexibility of having a staging area that can be compromised in order to conduct research can be an invaluable tool in threat assessment, and security policy testing. A lab also offers an incredible training tool for any information security professional. Using older equipment also has several advantages, namely, reduced cost, and slower systems can be dramatically affected under heavy loads, making it easier to evaluate the impact of threats.

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

Setting up a test lab, and the related research done using the lab may be tax deductible as an “employee education” expense, or may be applicable for research and development grants. (10)

© SANS Institute 2003, Author retains full rights.

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

WORKS CITED

(1) Sission, Derek. A thoughtful approach to web site quality. . January 7th, 2003 http://www.philosophe.com/testing/testsuite.html.

(2) Bailey, Don. Attack Lab Design & Security Mini How-To. . January 7th, 2003 http://ruff.cs.jmu.edu/~beetle/download/attacklab.html#B.

(3) Hart, Baker . Building a Security Lab with Virtual Machines. GIAC. January 7th 2003 http://www.giac.org/practical/Edwin_Hart_GSEC.doc.

(4) Components of the Virtual Network. VMWare Inc. January 7th, 2003 http://www.vmware.com/support/ws3/doc/ws32_network2.html#1008276.

(5) Autoview 200/400 Installation / Users Guide. : Advocent Corporation, 2002

(6) Norton Ghost Users Guide. United States of America: Symantec, 2002.

(7) F-Secure Virus Descriptions - Klez. Fsecure Anti Virus Research Team. January 7th, 2003 http://www.europe.f-secure.com/v-descs/klez.shtml.

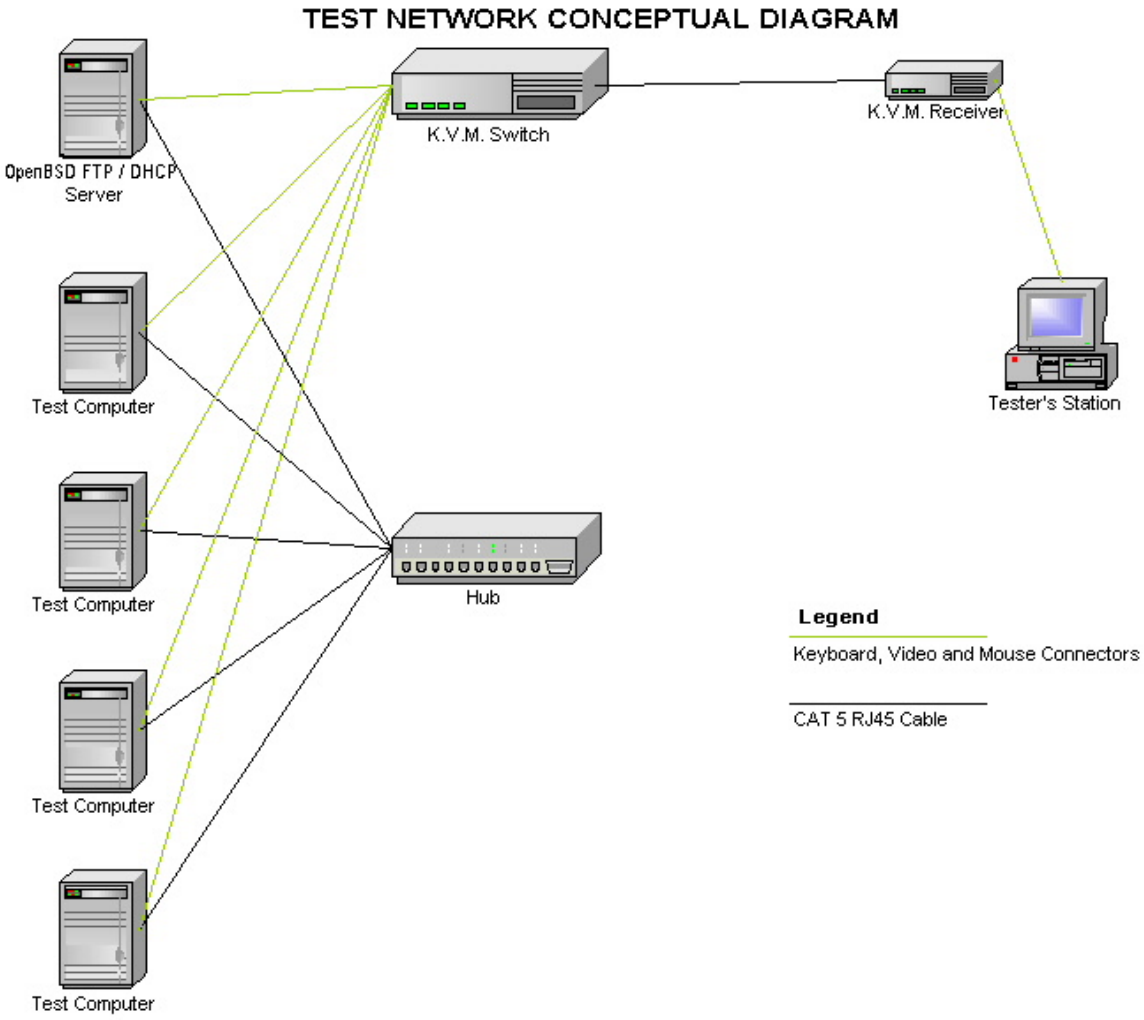
(8) Feyrer, Hubert. G4U - Harddisk Image Cloning for PCs. . January 7th, 2003 http://www.feyrer.de/g4u/.

(9) Herberlein, Todd and Bishop, Matt. An Isolated Network for Research. Department of Computer Science, University of California at Davis. January 7th, 2003 http://seclab.cs.ucdavis.edu/papers/bishop,heberlein-1996.pdf.

(10) Trewolla, John. An Inexpensive Personal Security Training Laboratory. The SANS Institute. January 7th, 2003 http://www.sans.org/rr/start/lab.php.

© SANS Institute 2003, Author retains full rights.

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



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