CHAPTER

Setting Up Your Lab

4

SOLUTIONS IN THIS CHAPTER

INTRODUCTION

> Дело право, толко гляди прямо. – Russian proverb: *"The shortest answer is doing."*
> **(Mertvago, 1995)**

For those who are interested in learning how to do *penetration testing* (or hacking, if you want to be "edgy") there are many tools available, but very few targets to practice safely against – not to mention legally. For many, learning penetration tactics has been through attacking systems on the Internet. Although this might provide a wealth of opportunities and targets, it is also quite illegal. Many people have gone to jail or paid huge amounts of money in fines and restitution – all for hacking Internet sites.

The only real option available to those who want to learn penetration testing legally is to create a penetration test lab. For many, especially people new to networking, this can be a daunting task. Moreover, there is the added difficulty of creating real-world scenarios to practice against, especially for those who do not know what a real-world scenario might look like. These obstacles often are daunting enough to discourage many from learning how to conduct a *PenTest* project.

This chapter and the next will discuss how to set up different penetration test labs, as well as provide scenarios that mimic the real world, providing the opportunity to learn (or improve) skills that professional penetration testers use. By creating a PenTest lab, we will be able to repeat hands-on penetration test exercises on real servers. We will also be able to conduct penetration tests against corporate assets in a safe environment, without impacting production systems.

PERSONAL LAB

The need for personal labs is high – even professional penetration testers set up small, personal labs at home to experiment on. There is a difference between a personal lab, and a professional lab that should be noted. A professional lab, even if maintained by an individual, can be used to identify and report on discovered vulnerabilities. For those readers who are interested in maintaining a professional lab, they should skip ahead to the section titled "Corporate Lab." This section will focus on creating a small lab for personal use, where different hacking techniques can be learned and replicated, but a lot of security features are relaxed. The primary objective of personal labs is almost purely educational and often used to replicate or create exploits. This is different than corporate labs, which are used to exploit corporate assets.

Keeping it simple

Cost is usually a driver in trying to keep personal labs small and manageable. Unless there is a need to include a lot of equipment, labs can reside on a single system using virtual machine (VM) applications. There is also no need to maintain a large library of applications. Open Source applications can be downloaded when needed, and systems can be reconfigured easily in small labs.

Unless a personal lab retains any sensitive data, a lot of security controls can be eliminated, including the security issues mentioned in this chapter. If wireless connectivity is used in the lab, access controls should stay in place, however.

Equipment

Although older computer equipment can be used in a penetration test lab, older equipment has additional costs not usually considered, including time and power. A personal lab that only focuses on application and Operating System (OS) hacking does not require any advanced networking equipment, but does require a more robust computing platform to handle multiple VMs running simultaneously. When conducting brute force attacks or password attacks, faster processing speed is beneficial – something that older systems cannot always provide. Although older systems are easier to come by (someone is always trying to give me their old computers), they may actually be more of a hindrance than a help.

TIP I have found that I can conduct all my application and OS penetration testing using just a decent laptop and VMware Player as the VM engine. In the past, I used older systems that could only run one image at a time, requiring me to maintain multiple systems; all those systems generated a lot of heat and consumed a lot of power. With today's technology, it only makes sense to look for cheaper and more eco-friendly alternatives.

Software

An advantage for anyone creating a personal lab is that in today's information technology environment, many applications used in corporate networks are Open Source, which are easy and free to obtain. Proprietary software, including OSes, is another matter. In personal labs, a tough choice needs to be made – stick with all Open Source applications, or purchase applications as needed. While Microsoft Developer Network has yearly subscriptions for many of the Microsoft products and may be a cost-effective alternative over the long run, older applications and OSes can still be purchased online. In some cases, trial versions may also be downloaded for free.

Unless there is a need to obtain proprietary software (such as replicate a newly discovered exploit), Open Source software is often sufficient to learn hacking techniques, including system, application, database, and Web attacks. Another option to obtaining software would be to visit VMware and download some prebuilt OS images containing applications at www.vmware.com/appliances/. These "virtual appliances" can be used as targets in a lab, and they also provide an opportunity to practice the penetration test methodologies described later in this book.

NOTE There are some other disadvantages to using Open Source tools – one of those being application support. The large commercial tools tend to have a support staff that will quickly respond to your questions and problems (they better, considering how costly they tend to be). Open Source tools do not usually have this type of support – rather most problems have to be searched for through wiki pages or various forums strewn about the Internet.

Lab for Book Exercises

In Part II of this book, we will use the following general configuration for our personal lab, as seen in Figure 4.1. As we can see, there are two pieces of hardware – a router and a computer. Even though Figure 4.1 shows a laptop and a wireless router, these are not a requirement; a wired router and a desktop will work as well. The OS on the computer will be Microsoft Windows. All LiveCDs will be run within a VM – for our examples we will use VMware Player.

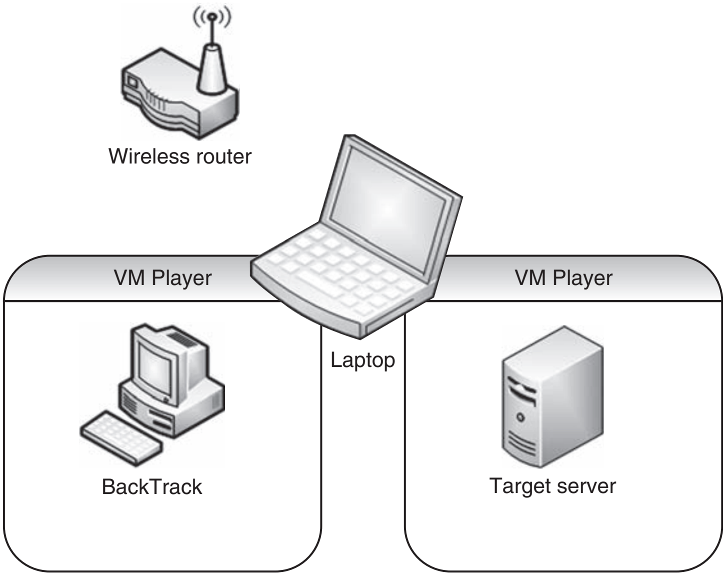


FIGURE 4.1

Lab Configuration

Here is a list of configuration information that can be replicated in any lab attempting to repeat the examples provided in the book.

Router configuration:

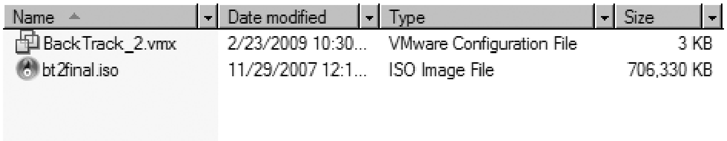
- Dynamic Host Configuration Protocol (DHCP) Server: active
- Pool Starting Address: 192.168.1.2
- Local Area Network Transmission Control Protocol/Internet Protocol (LAN TCP/IP):
  - IP Address: 192.168.1.1
  - IP Subnet Mask: 255.255.255.0

Computer configuration:

- 400 MHz or faster processor (500 MHz recommended)
- 512MB random access memory (RAM) minimum (2GB RAM recommended)

VM:

- VMware Player
- Available at: www.vmware.com/products/player/



Name	Date modified	Type	Size
BackTrack_2.vmx	2/23/2009 10:30...	VMware Configuration File	3 KB
bt2final.iso	11/29/2007 12:1...	ISO Image File	706,330 KB

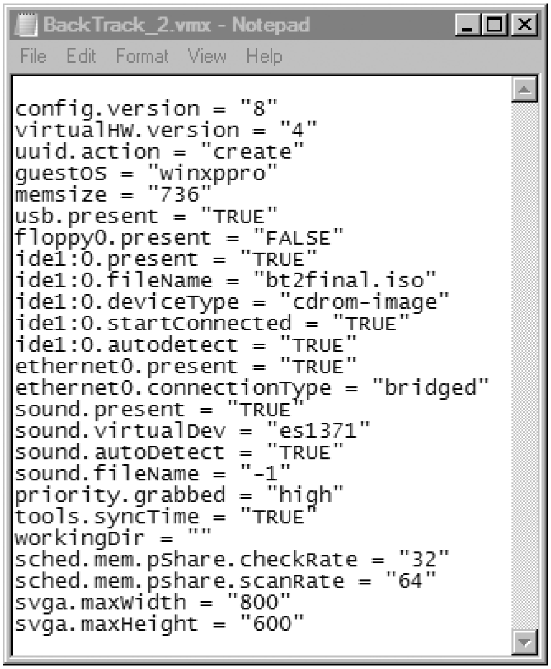
FIGURE 4.2

Directory Containing ISO and VMX file

Each LiveCD, including the BackTrack image, are provided on the DVD as an International Organization for Standardization (ISO) disk image. In the case where the use of LiveCDs is preferred, the ISO images can be used to create CD versions of the De-ICE LiveCD servers, using DVD burner software.

The most convenient way to set up a lab is to use the ISO images along with a .VMX file, which is included on the DVD. To use the VMX file with the ISO disk image, both files need to be in the same directory, as seen in Figure 4.2.

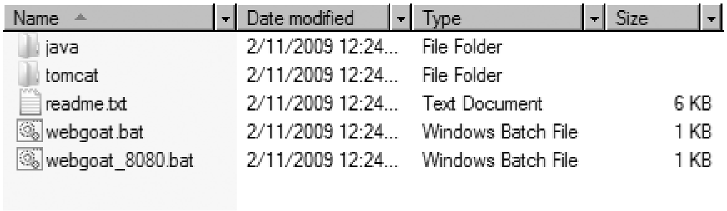
If VMware is installed, the Microsoft OS will recognize the VMX file as a VMware configuration file. Launching the VMX file will run the ISO file within VM Player. In Figure 4.3, the contents of the VMX file are listed. The line *ide1:0.fileName = "bt2final.iso"* can be modified to match the ISO file name.



```
config.version = "8"
virtualHW.version = "4"
uuid.action = "create"
guestOS = "winxppro"
memsize = "736"
usb.present = "TRUE"
floppy0.present = "FALSE"
ide1:0.present = "TRUE"
ide1:0.fileName = "bt2final.iso"
ide1:0.deviceType = "cdrom-image"
ide1:0.startConnected = "TRUE"
ide1:0.autodetect = "TRUE"
ethernet0.present = "TRUE"
ethernet0.connectionType = "bridged"
sound.present = "TRUE"
sound.virtualDev = "es1371"
sound.autoDetect = "TRUE"
sound.fileName = "-1"
priority.grabbed = "high"
tools.syncTime = "TRUE"
workingDir = ""
sched.mem.pShare.checkRate = "32"
sched.mem.pshare.scanRate = "64"
svga.maxWidth = "800"
svga.maxHeight = "600"
```

FIGURE 4.3

VMX File Content



Name	Date modified	Type	Size
java	2/11/2009 12:24...	File Folder	
tomcat	2/11/2009 12:24...	File Folder	
readme.txt	2/11/2009 12:24...	Text Document	6 KB
webgoat.bat	2/11/2009 12:24...	Windows Batch File	1 KB
webgoat_8080.bat	2/11/2009 12:24...	Windows Batch File	1 KB

FIGURE 4.4

WebGoat Directory

In the case of WebGoat, the application was not designed to be run in a VM. For this book, we will run WebGoat on the computer system itself. Figure 4.4 shows a snapshot of the files and directories used by WebGoat. As we can see, there are two batch files that launch WebGoat.

The files and directories are in a zipped file, which is available on the accompanying DVD or downloadable at http://code.google.com/p/webgoat/. The history and documentation for WebGoat can be found at www.owasp.org/index.php/Category:OWASP_WebGoat_Project. The zip file can be extracted into any directory on the computer system (indicated as the laptop in Figure 4.1). Once extracted, either of the bat files can be executed, which will be demonstrated in Chapter 11.

CORPORATE LAB

Many companies still do not see security as a way to improve profits and are not willing to establish corporate-level penetration testing teams. These organizations often simply contract out for security audits, and they may or may not contract out for penetration tests. However, a large number of corporations are adopting a different view, and they are creating risk assessment groups to evaluate corporate assets. This section will discuss PenTest labs that have corporate backing.

Corporate labs have a different function than personal labs. The objective of personal labs is often purely educational. Corporate labs are systems that contain hacking tools of all kinds, so that the penetration test engineers can attack corporate assets, looking for exploitable vulnerabilities. There is an expectation that PenTest engineers already know how to conduct attacks and compromise vulnerabilities, so practice labs are rarely created. In cases where the engineers need to test exploits, test networks that mirror production networks are usually made available to the PenTest team.

Maintaining and patching systems that scan and attack corporate assets is essential and usually mandated by corporate policy. Beyond patching, system access must be strongly controlled. Information gathered during a penetration test is extremely sensitive, and unauthorized access to the collected data could jeopardize not only the target system but also the corporation as a whole. There are many different methods that can be used to prevent unauthorized access to corporate penetration test lab systems, including firewalls, access controls, and one-time passwords. The exact architecture surrounding PenTest systems will differ depending on the business needs of the company and sensitivity of the data collected during a penetration test.

Internal Labs

There isn't much difference between internal and external penetration test labs with regard to hardware and software. The difference between the two groups is accessibility. Internal labs are placed within the corporation's intranet, which usually has fewer restrictions regarding access to network assets and servers. Penetration tests within a corporate network often yield greater successes than external PenTests, primarily because there is a pervasive viewpoint among system administrators that company employees should be trusted.

The purpose behind internal penetration tests is to identify vulnerabilities that are susceptible to attack from the "insider threat." Insider attacks are not attributable only to employees – contractors and vendors who have access to internal servers are all part of the insider threat.

> **NOTE** Although Hollywood likes to use evil hackers breaking into corporate networks in movie plots, reality is quite different. Most attacks (intentional or not) come from employee or contractor systems and are launched from within the corporate network – not externally. Penetration testing should include both internal and external penetration testing to assure all security vulnerabilities are identified.

External Labs

In external PenTest projects, the objective is to identify ways to penetrate through various obstacles (such as firewalls and intrusion detection systems [IDSes]) in the network, and gaining access to systems behind these defenses. To accomplish this task, penetration test systems need to be placed in an external network. Often, systems are placed in a separate *demilitarized zone*, so that access to the PenTest lab systems is restricted, yet access to corporate assets is similar to that of any Internet-connected system.

Equipment

The equipment necessary to conduct internal or external penetration tests varies, depending on the size and needs of the corporation. Generally, multiple platforms will be used to host different applications, such as vulnerability identification applications, vulnerability exploitation platforms, Web scanners, and other general hacking tools. In cases where remote brute force attacks are conducted, bandwidth constraints must be addressed. Corporate penetration testers can also benefit from access to servers that have high processing capabilities, especially if any password or encryption cracking needs to be performed.

Physical access to PenTest equipment should be controlled. Lab devices should not be accessible to anyone, other than those on the PenTest project. It is much easier to gain access to a system when physical access is possible, so physical security should be evaluated and strengthened according to data sensitivity.

Software

There are many commercial and Open Source tools available to penetration testers that will help speed up and improve the accuracy of a penetration test. A list of tools is available at www.sectools.org. We will discuss some of the tools listed on the sectools.org Web site throughout Part II of this book and use both commercial and Open Source tools in the chapter examples.

Which tools to use depends on the purpose of the penetration test, business needs, and budget – in large organizations, it is not unusual to include a variety of applications to cover all type of penetration tests, including applications designed for network, system, database, and Web attacks.

PROTECTING PENETRATION TEST DATA

During a penetration test, engineers gain access to client data that could be very sensitive in nature. It is imperative that collected client data is protected during the course of the PenTest. This section will discuss some of the challenges and solutions to securing client data and the penetration test systems used by small and large organizations.

Encryption Schemas

In a PenTest lab, many different types of OSes and software applications are used. It is important to store these disks in a secure manner for the following two reasons: (1) disks grow invisible legs and "walk out" of the lab (intentionally, or not), and (2) integrity of the data on the disks is critical.

Data Encryption

With regard to install disks "walking out," anyone who has had to support a network finds themselves short of disks. Sometimes it is because people borrow them, or the network administrators forget and leave disks in CD trays. Although it may not seem serious, loss of software is often indicative of weak procedures and controls, which can threaten the credibility of a penetration test team. If any installation disk containing third-party applications or OSes leaves the penetration test lab, the risk of sensitive data loss may be low. However, if the installation disk contains sensitive information, such as proprietary software code or configuration information, the loss of data could be financially damaging.

To prevent any losses from becoming a corporate disaster, all data should be encrypted as feasibly as possible. This includes data at rest on lab systems – equipment can also "walk out" just as easily as install disks. Enforcing encryption on all at-rest data places additional responsibility on the lab engineers, since encryption keys must be properly secured.

Additional encryption methods to consider include hard drive encryption and Basic Input/Output System (BIOS) password protection. Applications exist that will encrypt a system's entire hard drive, which will protect the data from unauthorized disclosure in case the hard drive (or entire system) is stolen. Although the loss of equipment can be costly, the loss of any sensitive data could be far worse.

BIOS password protection also reduces the risk of a malicious user accessing system data, especially on laptops. A system can be configured to require the BIOS password before booting, effectively preventing unauthorized users from accessing the system.

Data Hashing

The issue of the install disk integrity is also a serious matter. Some OS and patch disks are delivered through well-defined and secure channels; but more often than not, patches and updates are downloaded directly over the Internet. How does a person who downloads software over the Internet know that what they are downloading is a true copy of the file and is not corrupted or maliciously altered? Hash functions.

All applications and software downloaded for use in a PenTest lab should be verified using a hash function. A *hash function* is a mathematical process where a file is converted into a single value. This value should be (theoretically) unique for each file. Any modification to a file, even just one bit, will dramatically change the hash value.

The most popular is MD5, and for those security-conscious software writers, there is usually a published MD5 value associated with each download. Once the PenTest team has downloaded a file, it is critical to verify that they have a true copy of the file by conducting an MD5 hash against it and comparing it to the author's published value. Once this is verified, the value should be recorded somewhere for future reference, such as a binder stored in a safe.

WARNING A program can have different hash values, depending on the OS it was compiled to run on. An MD5 hash in one Linux distribution might be different in another distribution, such as Microsoft Windows. It is important to keep track of which OS distribution you are using when you record the hash.

MD5 hashes should also be used on any install disks, to validate that the proper disks are being used, especially before they are used in the PenTest lab. This provides the PenTest team confidence that what they are using is a true copy of the file. Verifying the hash can provide a mechanism for detecting when the wrong version of an application is being considered for use in a lab. By comparing the MD5 hash of an application against a printed list, it quickly becomes obvious if the wrong disk or file was chosen to be used in the lab. This extra validation step is a valuable safeguard against innocent mistakes if the wrong software is used by accident.

Securing PenTest Systems

As a best practice, all computers need to have safeguards that are at least equal to the value of the data that resides on it. The minimum level of protection needed to secure your system should be outlined by your corporate policy. However, it is almost always acceptable to go beyond this minimum level. In cases where it does not seem the corporate policy is sufficient, here are some suggestions that can improve your protection:

- Encrypt the hard drive: In the later versions of Microsoft Windows, files, directories, and even the entire hard drive can be encrypted. However, understand that there is more than one way to decrypt the drive – computer encryption is often controlled by the corporation, and they usually have a way to decrypt your computer as well. Key management is critical, and is hopefully in the hands of people as paranoid as penetration testers.
- Lock hard drives in a safe: If hard drives can be removed from the work computer, putting the drives in a safe is a great way to protect them. In the event of physical disasters, such as a fire or earthquake, the hard drives may come out of the disaster unscathed (depending on the quality of the safe, of course). If the work computer is a laptop, just keep the entire laptop in the safe. Laptops used onsite at a client's facility should be constantly secured and should never be left unattended. Leaving the laptop in a car should never be considered a method of protection.
- Store systems in a physically controlled room: A PenTest lab should be located in a separate room with physical security controls in place to restrict access to unauthorized personnel. In many larger organizations, test labs are separated and located behind key-controlled doors. However, in many cases, the penetration test lab occupies space with servers from various departments. This can pose a problem; people who have legitimate access to these other servers should probably not have physical access to the penetration test servers, since they might contain data more sensitive in nature than other systems in the same room.

- Perform penetration tests against the PenTest systems: What better way to know if the PenTest systems are vulnerable to attack than to actually attack them. Naturally, backups need to be made (and secured properly) beforehand, and sanitization procedures performed afterwards.

Are You Owned?

Backups can be Infected

One of my worst experiences was dealing with the *Blaster Worm*. The company I worked at had been hit hard, and it took a long time to clean up the network. What was worse, though, is we kept being infected at least once a month for almost a year, and neither the network nor the security team could figure how Blaster kept getting through our defenses. Later on, we found out that the production lab had created copies of various infected servers to use as "ghost" images, which can be used to quickly restore a server. Although a great time-saver for the lab team, every time they brought up a server using an infected ghost image, the network was hammered.

Mobile Security Concerns

A lot of penetration tests are conducted near or on the client's property. With today's mobile technology, a lot of these penetration tests include examining wireless networks. In a penetration test involving a wireless network (or any network for that matter), the first thing that must happen is the PenTest team needs to gain access to the network. It really does not matter if it is over the wireless portion of the network, or a plug in the wall. All that matters is that access is established. When access occurs over wireless, an additional risk is created – interception of sensitive data. In some cases, client wireless access points do not use strong encryption methods to secure data transmitted to connecting clients. If a penetration test involves accessing wireless access points, it is best if wireless access is limited and used only when necessary. Once wireless network access is accomplished, the penetration testers should try and relocate that access to a wired network where additional safeguards can be implemented.

Another security issue related to mobile computing is access to PenTest systems. In larger corporations, PenTest systems are permanently placed in internal and external networks across disparate geo-locations, so that the penetration tester can remotely attack assets. This provides a better understanding of what risks exist from internal and external threats, so that security measures can be applied appropriate to threats. Access to remote PenTest systems need to be managed using strong security controls. Network PenTest systems should be placed in secure networks with limited external access; virtual private networks can be used to control access to the network, yet still permit penetration test engineers access to their systems so they may launch their attacks.

Wireless Lab Data

A penetration test lab may include wireless access points to provide the PenTest engineers an environment to test wireless hacking techniques. In cases where wireless access points are desired, it is important to secure systems within the lab, since access to wireless signals extend beyond walls and floors. To protect systems from unauthorized access, two separate labs should be created – a wireless lab designed to practice wireless hacking, and a separate lab that can be used to conduct system attacks. The wireless lab should only be used to train on wireless hacking techniques or to perform tests on custom configurations.

In those situations where there are multiple wireless access points in the vicinity of your wireless lab, utmost care is required to make sure access to the lab's wireless network is controlled, using strong encryption and strong authentication methods, at a minimum. Current technology, such as Wi-Fi Protected Access (WPA2), should be standard practice in setting up and running a wireless penetration test lab. Strong security and an isolated wireless network not only protect the data within the penetration test lab, it also protects anyone accidentally connecting to the lab, especially in those instances where viruses, worms, or botnets are being used for testing purposes.

Tools and Traps...

Dangers in Autoconnecting

I set up a wireless lab at my home not too long ago. It turned out that the local police department next door to my apartment had the same wireless configuration that I intended to use for testing purposes. After further review, I realized the police department set up their wireless access point with no encryption. Had I just plopped in my BackTrack LiveCD and started to hack away, there was a good chance I would have been hacking the police network, instead of mine. I am not sure they would have taken kindly to my activities.

ADDITIONAL NETWORK HARDWARE

In a corporate environment, network hardware is often included within a penetration test during network assessments. In production networks, attacking network appliances (such as routers, IDSes, firewalls, and proxies) can sometimes result in network crashes or denial of service (DoS) of network servers. In cases where there is a risk to the network, PenTest projects often break their attacks up into two different scenarios. The first scenario is to attack test networks that are identical to the production network. This allows the penetration test engineers to conduct more aggressive attacks (including brute force and DoS attacks), and allows the network administrators to monitor the impact that the PenTest has on the network. After the test network has been sufficiently tested, the knowledge learned from attacking the test network is then used against the production network, with the exclusion of the more aggressive attack methods.

For personal penetration test labs, access to network devices is much more problematic than in the corporate world. To practice hacking and evasion techniques against network devices, hardware purchase are often required. If the only objective in a personal lab is to learn how to attack applications and the OS, network hardware can be ignored. However, to understand all the nuances involved in network hacking, there really isn't any other choice than to purchase hardware.

NOTE Even though network configuration seems to be outside the topic of penetration testing, understanding how to read configurations and learning what the "best practices" in designing networks is extremely helpful in a penetration test involving network devices. As we discussed in Chapter 3, penetration testers with a network architecture background can identify deficiencies in a large variety of network designs, which may be the key to a successful penetration test project.

Routers

Router attacks are probably the most prevalent type of attacks in network penetration tests. Inclusion of routers and switches in the PenTest lab would provide an additional educational facet to network attacks, including router misconfigurations, network protocol attacks, and DoS attacks. Home routers are not good choices to include in a personal lab since they are simply stripped down versions of real network devices.

Which routers to purchase is a personal choice, depending on what Network Architecture career path has been chosen. Companies that provide certification in networking are a good source of information as to which routers to select. For example, in selecting a Cisco or Juniper certification, it would be prudent to obtain the routers suggested for the Cisco Certified Network Professional (CCNP) or the Juniper Networks Certified Internet Specialist (JNCIS-ER). If money is not an object, then obtaining the suggested Cisco Certified Internetwork Expert (CCIE) or Juniper Networks Certified Internet Expert (JNCIE-ER) lab equipment would make the most sense.

Firewalls

Firewall evasion is an advanced skill that needs practice. Part of the difficulty is identifying when the firewall is preventing access to a back-end system, and when the system itself is the obstacle. Stateful and stateless firewalls present different problems as well, which again takes practice to identify and overcome.

Network firewall devices can be obtained from commercial vendors, such as Cisco, Juniper, Check Point, and others. There are some Open Source alternatives, including client firewalls (such as netfilter/iptables). The Open Source alternatives provide a realistic target, and have the additional advantage of being free. The advantage to obtaining devices from vendors is that familiarization with the different configurations on commercial firewalls can help in corporate penetration tests, since Open Source firewalls are rarely seen in large organizations.

It is not necessary to purchase high-end firewalls for the penetration test lab. Low-end vendor firewalls contain the same OS and codebase as the high-end firewalls. Often, the difference between the cheaper and more expensive vendor appliances is the bandwidth.

Intrusion Detection System/Intrusion Prevention System

IDS and intrusion prevention system (IPS) evasion is helpful in the beginning stages of a penetration test. Eventually, the PenTest team will try to trigger the IDS/IPS systems to alert network administrators to the team's hacking attempts, but initially the PenTest team will try and obtain as much information as possible without being noticed in order to test the client's incident response procedures.

Probably the most widely used IDS/IPS system is the Open Source software application called *Snort*, which can be obtained at www.snort.org. Many of the rules used to detect malicious activity on the network target virus and worm activity. However, there are rules designed to detect hacking attempts, such as brute force attacks, and network scanning. Understanding "event thresholding" and learning to modify the speed of an attack can help in successfully completing professional penetration tests.

SUMMARY

In this chapter we discussed some of the general concepts surrounding PenTest labs, including personal and corporate labs. The primary purpose of personal labs is for education, which can be used to recreate exploitations against both proprietary and Open Source software and OSes. We will use a personal lab for the examples within this book and the accompanying DVD using VMs. If VM software is not an option, the LiveCDs can be burned onto CD media and used on systems within a physical lab. In Chapter 5, we will cover the use of the LiveCDs within the lab in greater detail.

Corporate labs, however, are used to identify system vulnerabilities within internal and external networks. There is an expectation that the engineers will already have the knowledge necessary to conduct penetration tests; in cases where testing is needed, test labs are preferred targets before any PenTesting is done against production servers.

Network devices can be added to a PenTest lab to provide additional realism and learning opportunities. With routers and switches, it is best to obtain commercial versions, since those designed for home use are often poor examples of those used in larger corporations. With firewalls and IDS devices, there are Open Source versions that can accurately mimic commercial appliances.

SOLUTIONS FAST TRACK

Personal Lab

- Cost is usually a driver in trying to keep personal labs small and manageable.
- Unless a personal lab retains any sensitive data, a lot of security controls can be eliminated.
- Open Source software is often sufficient to learn hacking techniques, including system, application, database, and Web attacks, unless there is a need to obtain proprietary software.

Corporate Lab

- The exact architecture surrounding PenTest systems will differ depending on the business needs of the company, and sensitivity of the data collected during a penetration test.
- The purpose behind internal penetration tests is to identify vulnerabilities that are susceptible to attack from the "insider threat."
- In external PenTest projects, the objective is to identify ways to penetrate past various obstacles (such as firewalls and IDSes) in the network and gaining access to systems behind these defenses.

Protecting Penetration Test Data

- All applications and software downloaded for use in a PenTest lab should be verified using a hash function to protect the PenTest assets and client information.
- PenTest systems often contain data that requires additional security controls. Corporate security policies may be insufficient.

Additional Network Hardware

- In production networks, attacking network devices can sometimes result in network crashes or DoS of network servers. It is prudent to conduct initial tests within a test network before targeting production networks.

- Routers can be introduced into a PenTest lab, which will allow network penetration techniques to be learned. Commercial routers and switches are preferred over those built for home use.
- Open Source firewalls can be used to learn firewall evasion techniques. Commercial firewalls are beneficial if the goal is to learn about commercial firewall configuration and potential misconfigurations that can be used to circumvent firewall protection in the network.
- The Snort IDS/IPS application is a valuable tool to use in a lab to learn how to modify the speed of network attacks to avoid detection.

FREQUENTLY ASKED QUESTIONS

Q: Are there any other VM software that can be used on a Linux system?

A: The Xen Hypervisor has been successfully used on Linux to host the De-ICE LiveCDs. Xen can be located at www.xen.org.

Q: Why should I care if I use a wireless access point in my lab, or if I use any encryption at all? If someone connects to it and their system is damaged as a result of penetration tests within the lab, it's their own fault for connecting to a network they don't have authorization to connect to.

A: The laws surrounding unauthorized access to wireless networks are still being written. The problem is that most wireless devices are configured to automatically connect to the strongest signal. If that signal is coming from the lab, the user may not even be aware that they have connected to a hostile network. Strong encryption can prevent accidents from happening.

Q: Should I be concerned with adding network devices to my lab if all I am interested in is Web hacking?

A: Probably not. However, the use of Web proxies in the network would provide an additional challenge and would also provide a more realistic scenario of what larger corporations do to protect their Web server. Adding network devices into a lab brings more realism into any PenTest scenario, and can improve the skills and knowledge of the PenTest engineer.

EXPAND YOUR SKILLS

Want to know about vulnerability verification? The following exercises are intended to provide you with additional knowledge and skills, so you can understand this topic better. Use your lab to conduct the following exercises.

EXERCISE 4.1

Creating a Personal Lab using VMware

1. Download the VMware player from VMware.com. Install the player on a Windows system that meets the requirements listed in this chapter.
2. Test the installation by downloading and running one of the prebuilt "virtual appliances" available through the VMware Web site at: www.vmware.com/appliances/. Do not close this VM.
3. Use the BackTrack ISO and VMX file included on the accompanying DVD and start the image by double-clicking on the VMX file. You should have two instances of VM Player running – the virtual appliance downloaded and launched in step 2, and the BackTrack image. If both systems are able to run without performance degradation, your system will work with the exercises provided in the book and with the video tutorials on the DVD.

EXERCISE 4.2

Expanding the Personal Lab with Network Devices

1. Query on an Internet Search Engine for "CCIE Lab Equipment." List which routers are recommended. Which switches are recommended? What Internetwork Operating System (IOS) is recommended?
2. Visit Snort.org, and obtain the "Snort Users Manual" from the Documentations section of the Web site. Identify the "Preprocessors" listed in the manual. What is Event Thresholding? What are the "three types of thresholding," and their frequency of alerts, according to the Snort manual?
3. Define "iptables" and "netfilter." What is the difference between the two?

REFERENCE

Mertvago, P. (1995). *The comparative Russian-English dictionary of Russian proverbs & sayings*. New York: Hippocrene Books.

This page intentionally left blank