22 Wrapping It Up

Throughout this book we have outlined and described many of the techniques we have found to be successful during penetration testing. As you perform penetration testing, you will develop new techniques and your own favorite tools. One of the most important points for performing adequate penetration testing is keeping your skills and tool kit current. The tools and techniques you use during testing need to be the latest and most up-to-date ones available. The people attacking your networks will be using the latest tools and techniques, so if you are not aware of such tools and have not tested your environment against them, you may be exposed. In this chapter we describe some ways to keep current on the latest tools and techniques in the industry.

Another important key to keeping your systems safe is the use of countermeasures. Throughout the book we have described countermeasures to specific tools or exploits. These countermeasures are on a more micro-scale; they address specific issues. While these types of countermeasures are important, there are larger, more broad-based countermeasures that can help prevent the smaller issues from occurring in the first place. A proper security architecture is a key element for keeping an organization secure. A security architecture includes policies and procedures, baseline standards, data classification, compliance and monitoring programs, and security awareness training.

22.1 COUNTERMEASURES

Throughout the book, we have identified countermeasures for many specific vulnerabilities. Closing specific holes, such as applying a patch to a Web server, addresses a real threat to security but does nothing to prevent a similar vulnerability from arising again in the near future. Often we perform penetration tests for clients and provide them with a long list of recommendations for fixing the issues we discover during testing. Frequently, the clients take action on the short-term, quick-fix issues but do little to address long-term problems. In these scenarios, the client's systems are relatively secure shortly after the testing was performed, but if we returned six months later, we would find many issues similar to those we discovered during the first test. Countermeasures must address both long- and short-term problems. Looking at the long-range picture, there are many tools for avoiding and preventing vulnerabilities, such as developing a security architecture as described above. We do not cover security architecture in depth since it is outside the scope of this book. However, we do highlight the importance of security architecture elements as countermeasures to computer security attacks.

Policies are important because they instruct personnel on proper procedures and acceptable use. Hopefully, the policies standardize procedures so that there is consistency in the environment. In addition, policies provide a basis for holding personnel accountable when they do not follow the standard set by the policy. You cannot expect personnel to act in a secure manner unless you define what you mean by "secure manner." One system administrator may think a "secure manner" includes writing passwords on sticky notes and keeping them on his or her desk. Another system administrator may think "secure manner" means users cannot connect to the Internet. Therefore, as much as possible, policies should define normal computer operations, acceptable uses, monitoring procedures, incident response procedures to follow in case of an actual incident, and other procedures. In addition, policies should be specific to groups. A system administrator and a normal user should not be governed by the same policies. Policies intended for system administrators should not be made available to the general population because they may reveal information that could be useful to an attacker. Finally, policies need to be updated regularly. Many times clients show us policies and procedures that are years out of date and the systems for which they were written no longer exist.

Minimum baseline standards are similar to policies. Baseline standards are specific configuration documents that delineate minimum configuration requirements that need to be in place on a specific type of system. Baseline standards should be developed for each system within the environment. For instance, an organization should have a minimum baseline standard for NT servers. Each NT server should be configured with a minimum account policy enforcing account lockouts, minimum password lengths, and other security settings. Each server should be built in accordance with these baseline standards or should have a waiver excusing the server from meeting the standard for a specific reason. Each type of system should have a baseline standard. Standards should exist for NT servers, NT workstations, UNIX systems, Web servers, and any other type of system. Different parameters with each standard should pertain to different classification levels. For instance, a high-risk asset may have an account lockout threshold of three attempts, whereas a low-risk asset's account lockout may be configured for ten attempts. Baseline standards start to bring consistency to an environment and help ensure security procedures are in place to prevent attack.

It is unrealistic to expect a company to protect a document containing a job-posting announcement as it would a directory containing the company's trade secrets. Organizations still need to operate effectively. If the security measures in place to protect an unimportant asset are too stringent and hamper productivity, the security measures are ineffective. Conversely, if the organization decreases security on the server containing the trade secrets to reduce the inconvenience to users, the measures are also ineffective. Data classification is important to determine which assets are critical and cannot afford to be compromised and which assets are less important and do not need to be guarded as closely. There are many means of data classification, but one common method includes classifying assets as high, medium, or low risk. The security procedures in place to protect each category of asset are different. This way the organization can concentrate on protecting critical assets and can loosen security requirements on less critical assets to help improve efficiency. Different policies and baseline standards should be tailored to correspond to each different level.

The use of data classification, policies, and procedures becomes less effective if the organization has no way to verify that the procedures are actually being followed. Compliance and monitoring programs involve verification through manual or automated means that standards and policies are being followed. The systems being tested should be compared against standards developed from the organization's policies, procedures, and baseline standards. Traditional methods of compliance and monitoring involve the use of an audit department. Many organizations' audit departments have neither the resources nor the expertise to conduct the highly technical audits necessary to ensure compliance with standards. Many automated tools are available to help with compliance and monitoring. Host-based assessment tools can help compare system configurations to standards and report deviations from standards. Many host-based assessment tools use an agent to review file permissions, open services, network settings, system policies, and other configuration settings that could affect the configuration of the systems. If, for example, a system administrator opens FTP on a critical server, the tool would report this change to the party responsible for compliance monitoring. Automated assessment tools can greatly decrease the personnel resources needed for a proper compliance program. However, automated tools can be costly and difficult to implement without proper expertise. Whether the methods used are automated or manual, a proper compliance and monitoring program is essential to an organization's security posture.

Security awareness training is another key element of a security architecture. Users and systems personnel need to be trained in proper procedures and the reasons for those procedures. Training should be tailored to the audience. Users should not receive the same security awareness training as system administrators. User training should focus on the key measures users need to take to increase the security of the organization, for example, areas such as password management, incident reporting, physical security measures, viruses and malicious code, and other security threats. Training for system administrators should concentrate on areas that they can influence: topics such as system standards, recognizing and reporting incidents, compliance and monitoring, and proper system procedures (for example, adding users, opening services, and applying patches). There are many other topics that should be included in training for users and administrators, but they are beyond the scope of this book. Without proper security awareness training, personnel may unknowingly create situations that harm the security of the organization. In addition, security awareness training helps the organization hold personnel accountable for violating security policies. Perpetrators will have trouble using a defense that they did not know the proper procedure or were not aware of a policy since the organization will have documentation that the person attended security awareness training.

However, security awareness training goes only so far. If an organization's security procedures are difficult to follow and significantly inconvenience the user, they will not be followed. For example, organizations that require users to remember ten different passwords for multiple systems are the ones that lead users to write their passwords on sticky notes and leave them on their desks. A single sign-on solution or other means of centralized authentication could make password management easier for users and thereby decrease the number of exposures created by users deviating from security procedures. Therefore, when an organization is designing a security solution, it should seek to implement procedures that are easy to follow and enforce. Such procedures will decrease user and administrator security exposures more than the greatest security awareness training for difficult security procedures.

22.2 KEEPING CURRENT

Security tools and vulnerabilities change every day. Each day new exploits are published and new tools and scripts posted or updated. Since the field changes so quickly, you need to develop ways to keep current. Here we describe some of the methods we use. We monitor key Web sites that provide security and vulnerability information, subscribe to security-related mailing lists, and read trade magazines and white papers. These sources provide information on new developments and exploits. By constantly monitoring these sources of information, we can incorporate new findings into our testing procedures. Organizations can use the information to safeguard their systems against the latest vulnerabilities, obtain new testing tools, and develop new procedures for security testing. Below we list some of the sites and mailing lists we have found useful.

22.2.1 WEB SITES

One of the keys to keeping current is to find the sites and lists where the best players in the industry discuss and publish the latest tools and techniques. There are many security sites on the Internet. Listed below are some of the sites we have found helpful.

- *www.attrition.org*—famous for its defaced Web page archive.
- *www.cert.org* —site of Carnegie Mellon's Computer Emergency Response Team (CERT). Contains security information and the latest CERT advisories.
- *www.ciac.org*—news and bulletins of the Computer Incident Advisory Capability of the Department of Energy.
- *www.esecurityonline.com*—tools, vulnerability database, news, and resources.
- *http://freshmeat.net/*—security tools and exploits.
- *www.L0pht.com*—security tools, advisories, and information.
- *www.Nmrc.org*—excellent NetWare site containing tools, information, and documents. Also has information on Web and NT security.
- *www.ntsecurity.net*—vulnerabilities, tools, and information.
- *http://oliver.efri.hr/~crv/security/*—general security site, news, exploits, mailing lists, and so on.
- *www.packetstormsecurity.com*—a great site for the latest tools and discussions.
- *www.phrack.com*—security exploits and news.
- *www.rootshell.com*—primarily a UNIX site for news and exploits.
- *www.sans.org*—System Administration, Networking, and Security (SANS) Institute news, white papers, and so on.
- *www.securityfocus.com*—security information, tools, vulnerability database, and Bugtraq mailing list.
- *http://slashdot.org/*—security news.
- *www.technotronic.com/*—a great site for security tools and documents.
- *http://infosyssec.com/*—security information and links.

22.2.2 MAILING LISTS

In addition to Web sites, mailing lists can provide useful information. Many of these lists provide insight into the latest trends and developments in the security arena. There are many excellent mailing lists available today. Below we highlight some of the lists we have found helpful.

8lgm (Eight Little Green Men)—majordomo@8lgm.org

This list contains information on UNIX exploits.

To join, send an e-mail to majordomo@8lgm.org, and in the text of your message (not the subject line) write:

```
subscribe 8lgm-list
```

Academic Firewalls—majordomo@net.tamu.edu

Texas A&M maintains this list for discussing firewalls and other security tools in the academic environment. Sometimes hackers are more open with their exploit information in an academic setting than a commercial one. This lists complements the commercial Firewalls list (see below).

To join, send an e-mail to majordomo@net.tamu.edu, and in the text of your message (not the subject line) write:

```
SUBSCRIBE Academic-Firewalls
```

Alert—request-alert@iss.net

ISS moderates this list for the discussion of security products, vulnerabilities, and IDSs.

To join, send an e-mail to request-alert@iss.net, and in the text of your message (not the subject line) write:

```
subscribe alert
```

Best of Security—best-of-security-request@suburbia.net

Best of Security is a collection site intended to gather the best security information from other sites. Users of the list are instructed to send to the list the best information they come across from other sites (if the information has not already been sent).

To join, send an e-mail to best-of-security-request@suburbia.net with the following text in the body of the message:

```
subscribe best-of-security
```

Bugtraq—listserv@netspace.org

This is the mailing list that compliments the famous Bugtraq Web site. The list is primarily intended as a detailed discussion of UNIX security vulnerabilities. In addition, the list also provides information concerning security advisories, patches, and general UNIX security information.

To join, send an e-mail to listserv@netspace.org, and in the text of your message (not the subject line) write:

```
SUBSCRIBE BUGTRAQ
```

Computer Emergency Response Team—cert@cert.org

CERT provides security-related advisories. The CERT mailing list provides the latest CERT advisories in e-mail format.

To join, send an e-mail to cert@cert.org, and in the text of your message (not the subject line) write:

```
I want to be on your mailing list.
```

Computer Incident Advisory Capability—ciac-listproc@llnl.gov

The Computer Incident Advisory Capability (CIAC) of the Department of Energy provides information on security awareness, training, and education. It also provides data on security trends and vulnerabilities. CIAC has several mailing lists, including the following:

- CIAC-BULLETIN, which provides advisory information and time-critical security information
- CIAC-NOTES for Notes, which provides information about computer security articles

To join, send an e-mail to ciac-listproc@llnl.gov, and in the text of your message (not the subject line) write either of the following, depending on which list you want to join:

```
subscribe ciac-bulletin last_name, first_name phone_number
subscribe ciac-notes last_name, first_name phone_number
```

You should receive an acknowledgment containing an address, initial PIN, and information on how to change either of them, cancel your subscription, or get help.

Computer Underground Digest—cu-digest-request@weber.ucsd.edu

Computer Underground Digest is a list intended to discuss issues in the hacker community. It can give you insight into what is going on in the hacker community to help you understand new developments and threats.

To join, send an e-mail to cu-digest-request@weber.ucsd.edu, and in the text of your message (not the subject line) write:

```
SUB CUDIGEST
```

Cypherpunks—majordomo@toad.com

This list discusses privacy issues on the Internet. This list normally has a lot of activity.

To join, send an e-mail to majordomo@toad.com, and in the text of your message (not the subject line) write:

```
SUBSCRIBE cypherpunks
```

Firewalls—majordomo@greatcircle.com

As the name suggests, this is a list for firewall issues and discussions. It is similar to the Academic Firewalls list except this list is intended for the commercial industry.

To join, send an e-mail to majordomo@greatcircle.com, and in the text of your message (not the subject line) write:

```
SUBSCRIBE firewalls
```

Information Systems Security Forum—listserv@etsuadmn.etsu.edu

Information Systems Security Forum (INFSEC-L) is a forum for information systems security professionals to discuss security-related issues. The list is unmoderated so e-mail immediately goes to the entire list. The list owner reviews all initial list requests in an effort to ensure only security professionals subscribe.

To join, send an e-mail to listserv@etsuadmn.etsu.edu, and in the text of your message (not the subject line) write:

```
SUB infsec-l your_name
```

Intrusion Detection Systems—majordomo@uow.edu.au

This list primarily discusses IDS-related issues. The list deals with information on IDSs, methods, tools, and advisories.

To join, send an e-mail to majordomo@uow.edu.au with the following text in the body of the message:

```
subscribe ids
```

Microsoft Security—microsoft_security-subscribe-request@announce.microsoft.com

This list provides information on the latest security news from Microsoft.

To subscribe, send an e-mail to microsoft_security-subscribe-request@announce.microsoft.com.

NT Bugtraq—listserv@listserv.ntbugtraq.com

This list is similar to the Bugtraq mailing list above except it is primarily intended as a detailed discussion of NT security vulnerabilities. In addition, the list also provides information concerning security advisories, patches, and general NT security information.

To join, send an e-mail to listserv@listserv.ntbugtraq.com, and in the text of your message (not the subject line) write:

```
SUBSCRIBE NTBUGTRAQ first_name last_name
```

NT Security—request-ntsecurity@iss.net

This list maintained by ISS is intended for discussing Windows-related security issues. The list is unmoderated so e-mail immediately goes to all subscribers.

To join, send an e-mail to request-ntsecurity@iss.net, and in the text of your message (not the subject line) write:

```
subscribe ntsecurity your_e-mail_address
```

Phrack—phrack@well.com

This list is associated with *Phrack* magazine, which is a magazine that discusses hacker and underground news and events. The list discusses issues similar to those found in the magazine.

To join, send an e-mail to phrack@well.com, and in the text of your message (not the subject line) write:

```
SUBSCRIBE Phrack
```

Privacy Forum—privacy-request@vortex.com

Privacy Forum discusses both technical and nontechnical privacy issues.

To join, send an e-mail to privacy-request@vortex.com, and in the text of your message (not the subject line) write:

```
information privacy
```

Risks—risks-request@csl.sri.com

This list discusses technology-related risks associated with computing environments.

To join, send an e-mail to risks-request@csl.sri.com, and in the text of your message (not the subject line) write:

```
SUBSCRIBE
```

SANS Institute—digest@sans.org

The SANS Institute provides several mailing lists. The first is the Network Security Digest that discusses security-related information. NewsBites provides information about the latest new stories in the information security community. Finally, NT Digest is intended to discuss Windows NT–related information.

To join, send an e-mail to digest@sans.org and in the subject line add:

```
subscribe Network Security Digest or
NewsBites subscription or
NT Digest
```

Sneakers—majordomo@cs.yale.edu

The Sneakers list is intended as a forum for discussing penetration testing and evaluations of firewalls and other security products. All discussions are intended to be about legal testing performed by security professionals.

To join, send an e-mail to majordomo@cs.yale.edu, and in the text of your message (not the subject line) write:

```
SUBSCRIBE Sneakers
```

Virus—listserv@lehigh.edu

The Virus list discusses issues related to virus events, prevention, and questions and answers.

To join, send an e-mail to listserv@lehigh.edu, and in the text of your message (not the subject line) write:

```
SUBSCRIBE virus-l your_name
```

Virus Alert—listserv@lehigh.edu

The Virus Alert list is intended to provide virus warnings and alerts.

To join, send an e-mail to listserv@lehigh.edu, and in the text of your message (not the subject line) write:

```
SUBSCRIBE valert-l your_name
```

WWW Security—www-security-request@nsmx.rutgers.edu

WWW-Security is the official list of the Internet Engineering Task Force (IETF) Web Transaction Security Working Group. The list discusses development of Internet security standards and information related to securing Web services.

To join, send an e-mail to www-security-request@nsmx.rutgers.edu, and in the text of your message (not the subject line) write:

```
SUBSCRIBE www-security your_e-mail_address
```