Conducting a Penetration Test on an Organization

Chan Wai

TABLE OF CONTENTS

DETAILS
Full name: Chan Tuck Wai **GIAC userID: twchan001** **Course: Security Essentials** **Version: First (Original Submission)** **Conference Location: Malaysia**

Abstract

This document is decided to give readers an outlook on how a penetration test can be successfully done on an organization. A methodology has been drawn out in this document to allow readers to be acquainted with the process that penetration testers go through to conduct a penetration test.

What is a Penetration Test?

Penetration tests are a great way to identify vulnerabilities that exists in a system or network that has an existing security measures in place. A penetration test usually involves the use of attacking methods conducted by trusted individuals that are similarly used by hostile intruders or hackers. Depending on the type of test that is conducted, this may involve a simple scan of an IP addresses to identify machines that are offering services with known vulnerabilities or even exploiting known vulnerabilities that exists in an unpatched operating system. The results of these tests or attacks are then documented and presented as report to the owner of the system and the vulnerabilities identified can then be resolved.

Bear in mind that a penetration test does not last forever. Depending on the organization conducting the tests, the time frame to conduct each test varies. A penetration test is basically an attempt to breach the security of a network or system and is not a full security audit. This means that it is no more than a view of a system's security at a single moment in time. At this time, the known vulnerabilities, weaknesses or misconfigured systems have not changed within the time frame the penetration test is conducted.

Penetration testing is often done for two reasons. This is either to increase upper management awareness of security issues or to test intrusion detection and response capabilities. It also helps in assisting the higher management in decision-making processes. The management of an organization might not want to address all the vulnerabilities that are found in a vulnerability assessment but might want to address its system weaknesses that are found through a penetration test. This can happen as addressing all the weaknesses that are found in a vulnerability assessment can be costly and most organizations might not be able allocate the budget to do this.

Penetration tests can have serious consequences for the network on which they are run. If it is being badly conducted it can cause congestion and systems crashing. In the worst case scenario, it can result in the exactly the thing it is intended to prevent. This is the compromise of the systems by unauthorized intruders. It is therefore vital to have consent from the management of an organization before conducting a penetration test on its systems or network.

The Process and Methodology

Planning and Preparation

In order to make the penetration test done on an organization a success, a great deal of preparation needs to be done. Ideally a kickoff meeting should be called between the organization and the penetration testers. The kickoff meeting must discuss matter concerning the scope and objective of the penetration test as well as the parties involved. There must be a clear objective for the penetration test to be conducted. An organization that performs a test for no clear reason should not be surprise if the outcome contains no clear result. In most cases the objective of a penetration test is to demonstrate that exploitable vulnerabilities exist within an organization's network infrastructure. The scoping of the penetration test is done by identifying the machines, systems and network, operational requirements and the staff involved. The form in which the results or outcome of the test is presented should also be agreed upon the penetration testers and the organization.

Another important agenda to discuss during the meeting is the timing and duration the penetration tests are performed. This is vital, as it will ensure that while penetration tests are being conducted, normal business and everyday operations of the organization will not be disrupted. Penetration tests may need to be run at particular times of day. There may be conflicts between the need to ensure that everything is tested and the need to avoid loading the network during periods of heavy and critical use. Penetration tests that involve the use of unusual network traffic may cause some systems on the network to crash. If this risk cannot be tolerated then some systems or networks may need to be excluded from the test. Penetration testers should spend adequate amount of time discussing the tests with the organization before drawing up a testing plan. No organizations will want their businesses to be affected as a result of a penetration test. If the issue of timing is not resolved properly, this could be catastrophic to an organization. Imagine doing a denial of service 'test' on a university on the day its students take their online examinations. This is an example of poor timing as well as lack of communication between the penetration testers and the university. Good planning and preparation will help avoid such bad practices.

One major decision to be made with the organization is whether the staff of that organization should be informed before a penetration test is carried out. Advising staff is often appropriate, but it can change their behavior in ways that will affect the outcome of the penetration test. On the other hand, choosing not to warn staff may result in them taking action that unnecessarily affects the organization's operation. For example, a security team might be expected to react to an attack by disconnecting from the external network cutting all access to it. If the aim is to assess the response of the security team or other operational units then clearly management must accept such a risk. Otherwise it may be appropriate to give specific instructions that no action is to be taken in response to the penetration test at the time and duration arranged.

A complete and adequate penetration test involves penetration testers conducting illegal activities on systems external or internal to an organization's network. Organizations must understand that penetration testers performing the tests in most

cases are breaking the law. It is also vital to make sure the organization understands that any information or data obtained during the penetration tests will be treated as confidential and will be returned or destroyed accordingly after the tests. Prior to any penetration test engagements legal documents protecting the penetration testers and their company must be signed. This is a very important and not to be missed out step to be taken before conducting any penetration test on any organization. Even if the penetration testers are staff conducting tests on their on systems and network, they should also obtain the relevant legal documents protecting them against any legal actions. This serves as a protection to penetration testers should anything go wrong during the tests. Accidents can happen and no penetration testers would like to be sued as a result of doing their job.

Information Gathering and Analysis

After doing the necessary planning and preparation with the organization (or target) the next step is to gather as much information as possible about the targeted systems or networks. There's a wealth of tools and online resources available for us to do the necessary information gathering.

If the intended target has an online website, this is a good place to start your information gathering. We should always remember that any kind of information gathered during this stage may prove useful to us in the other stages of the penetration test. Information is power. A very good online resource is available at http://www.netcraft.com. The people at Netcraft have developed a service that has made our information gathering quite simple. Their service examines a network connected to the Internet and reports back which hosts are visible. It also gives you information like the operating it is running on as well as the server's uptime. Results of a probing on http://www.sans.org are shown in Appendix A.

The above method shown is an example of how information gathering can be done. Another more complete method is to do a network survey. A network survey serves as an introduction to the systems that are to be tested. The goal here is to find the number of systems that are reachable. The expected results that should be obtained from a network surveying should consist of domain names, server names, Internet service provider information, IP addresses of hosts involved as well as a network map. A network survey will also help us to determine the domain registry information for the servers. This allows us to check and see the range of IP addresses that are owned by the targeted organization.

A very useful tool to conduct a network survey is Nmap. Nmap is a tool made for scanning large networks. We could also use Nmap to determine what operating systems are running on a network as well as the type of packet filters/firewalls are in use, and numerous other characteristics.

Nmap is a tool not to be missed out and should be included in any penetration testers toolkit. The figure below shows a GUI version of Nmap that runs on Linux.

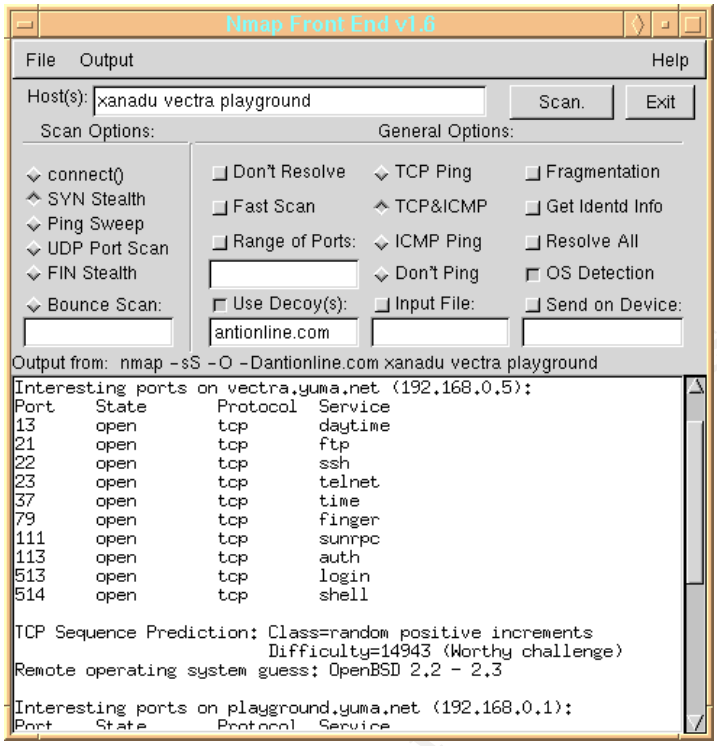

Figure 1: NMap (Source: http://www.insecure.org/nmap/index.html)

Upon doing a network survey and obtaining adequate information about the network the next task to be done would be to do a port scanning to obtain information about closed and open ports running on the systems or network. At this point, if there are any restricted IP addresses that the organization does not want the penetration tests be conducted on, the port scanning should not be performed on it. Make sure the IP addresses belong to the organization (one way is to compare domain registry information). There are basically about 65,000 possible TCP and UDP ports. Nmap is also a tool that can do port scanning. The figure above actually shows open ports that are available on a system. The basic results obtained from a port scan are a list of open ports on a particular IP addresses. At this point system information like the operating system should also be associated with the IP address. Nmap can help us obtain this information by conducting an OS fingerprinting. A good documentation on this and other uses of Nmap can be obtained from http://www.insecure.org/nmap/nmap-fingerprinting-article.html.

Of course there are other tools to help us conduct our information gathering and analysis. Some of these tools are listed in Appendix B. Most of the tools listed in Appendix B are free tools available to be downloaded from the Internet. The ideal result of the information gathering and analysis stage should be a list of systems and IP addresses with information about the operating system, running services and open ports.

Vulnerability Detection

After having gathered the relevant information about the targeted system, the next step is to determine the vulnerability that exists in each system. Penetration testers should have a collection of exploits and vulnerabilities at their disposal for this purpose. The knowledge of the penetration tester in this case would be put to test. An analysis will be done on the information obtained to determine any possible vulnerability that might exist. This is called manual vulnerability scanning as the detection of vulnerabilities is done manually. There is an exploit known as the dot bug that existed in MS Personal Web Server back in 1998. This is a bug that existed in IIS 3.0 that allowed ASP source code to be downloaded by appending a '.' to the filename. Microsoft eventually fixed this bug but they did not fix the same hole in their Personal Web Server at that time. Some Personal Web Servers has this vulnerability until today. If a system running Windows 95 and MS Personal Web Server pops up in the information gathered earlier, this would probably be a vulnerability that might exist in that particular system.

There are tools available that can automate vulnerability detection. Such a tool is Nessus (http://www.nessus.org). Nessus is a security scanner that audit remotely a given network and determine whether vulnerabilities exists in it. It produces a list of vulnerabilities that exist in a network as well as steps that should be taken to address these vulnerabilities. A screen shot is shown below: -

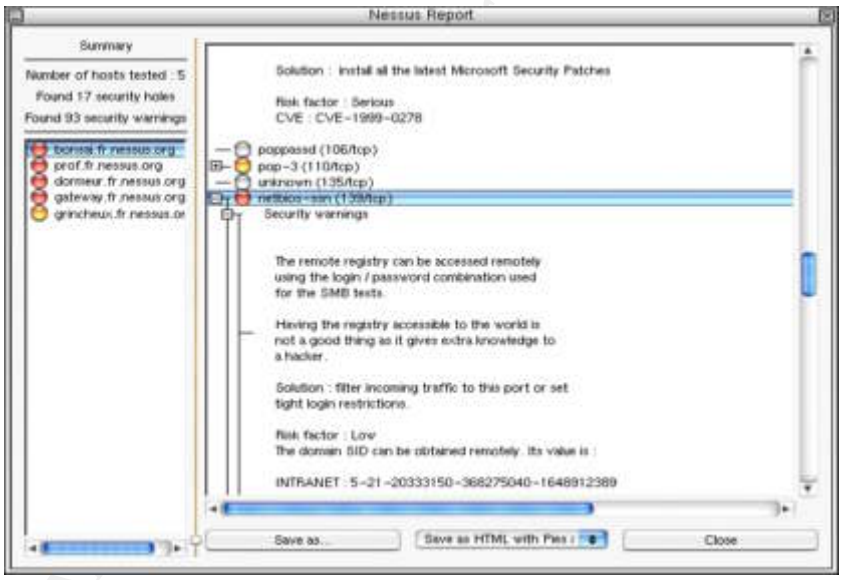

Figure 2: Nessus (Source: http://www.nessus.org)

The completion of the vulnerability detection will produce a definite list of targets to investigate in depth. These lists of targets will be used in the next stage. A penetration will be attempted at these targets that have their vulnerabilities defined.

Penetration Attempt

After determining the vulnerabilities that exist in the systems, the next stage is to identify suitable targets for a penetration attempt. The time and effort that need to put in for the systems that have vulnerabilities need to be estimated accordingly. Estimations on how long a penetration test takes on a particular system are important at this point. The target chosen to perform the penetration attempt is also important.

Imagine a scenario whereby two penetration testers are required to perform a penetration test on a network consisting of more than 200 machines. After gathering sufficient information and vulnerabilities about the network, they found out that there are only 5 servers on the network and the rest are just normal PCs used by the organization's staff. Common sense will tell these them that the likely target would be these 5 servers.

One practice that most organizations do is to name their machines in a way that they understand what the machine does. The computer name of the target is sometimes a decisive factor for choosing targets. Often after a network survey you would find computer names like SourceCode_PC, Int_Surfing and others that give penetration testers an idea of what the machine does. By choosing their target properly, penetration testers will not waste time and effort doing any redundant job. Normally penetration tests have a certain time constraint and penetration testers should not waste any time unnecessarily. There are other ways to choose a target. The above just demonstrates some criteria used.

After choosing the suitable targets, the penetration attempt will be performed on these chosen targets. There are some tools available for free via the Internet but they generally require customization. Knowing that a vulnerability exist on a target does not always imply that it can be exploited easily. Therefore it is not always possible to successfully penetrate even though it is theoretically possible. In any case exploits that exist should be tested on the target first before conducting any other penetration attempt.

Password cracking has become a normal practice in penetration tests. In most cases, you'll find services that are running on systems like telnet and ftp. This is a good place to start and use our password cracking methods to penetrate these systems. The list below shows just some of the password cracking methods used: -

- Dictionary Attack – Uses a word list or dictionary file.
- Hybrid Crack - Tests for passwords that are variations of the words in a dictionary file.
- Brute Force - Tests for passwords that are made up of characters going through all the combinations possible.

There's a very good tool that can be used to automate telnet and ftp account cracking. This tool is called Brutus (http://www.hoobie.net/brutus). The screenshot for this program is shown below: -

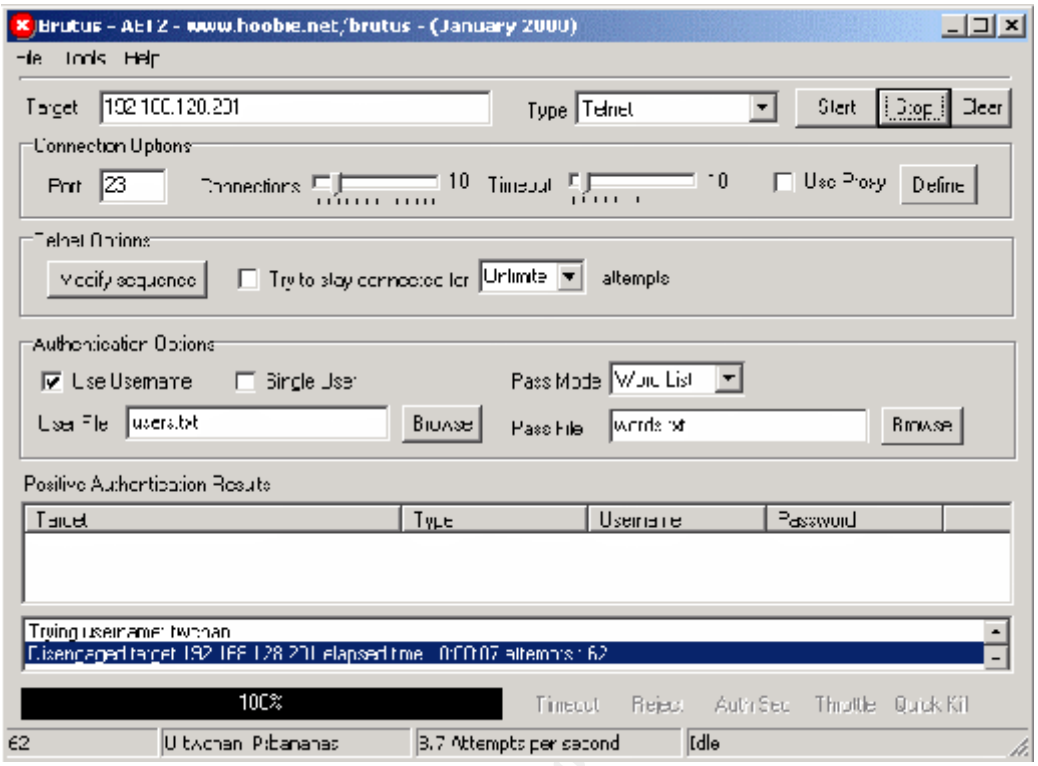

Figure 3: Brutus (Source: http://www.hoobie.net/brutus/)

The penetration attempts do not end here. There are two more suitable methods to attempt a penetration. This is through social engineering and testing the organization's physical security. Social engineering is an art used by hackers that capitalizes on the weakness of the human element of the organization's defense. The dialog below shows an example how an attacker can exploit the weakness of an employee in a large organization.

Attacker: "Hi Ms Lee, this is Steven from the IS Department. I've found a virus stuck in your mail box and would like to help you remove it. Can I have the password to your email ? "

Ms Lee (the secretary): "A virus ? That's terrible. My password is magnum. Please help me clean it up"

There's no harm in deploying social engineering and using it numerous times to obtain critical information from the organization's employees. This of course is bound to the agreement that the organization allows such methods to be used during the penetration tests. Physical security testing involves a situation of penetration testers trying to gain access to the organization's facility by defeating their physical security. Social engineering can be used to get pass the organization's physical security as well.

Analysis and Reporting

After conduction all the tasks above, the next task ahead is to generate a report for the organization. The report should start with an overview of the penetration testing process done. This should be followed by an analysis and commentary on critical vulnerabilities that exist in the network or systems. Vital vulnerabilities are addressed first to highlight it to the organization. Less vital vulnerabilities should then be highlighted. The reason for separating the vital vulnerabilities from the less vital ones helps the organization in decision making. For example, organizations might accept the risk incurred from the less vital vulnerabilities and only address to fix the more vital ones. The other contents of the report should be as follows: -

- Summary of any successful penetration scenarios
- Detailed listing of all information gathered during penetration testing
- Detailed listing of all vulnerabilities found
- Description of all vulnerabilities found
- Suggestions and techniques to resolve vulnerabilities found

Cleaning Up

The cleaning up process is done to clear any mess that has been made as a result of the penetration test. A detailed and exact list of all actions performed during the penetration test must be kept. This is vital so that any cleaning up of the system can be done. The cleaning up of compromised hosts must be done securely as well as not affecting the organization's normal operations. The cleaning up process should be verified by the organization's staff to ensure that it has been done successfully. Bad practices and improperly documented actions during penetration test will result in the cleaning up process being left as a backup and restore job for the organization thus affecting normal operations and taking up its IT resources.

A good example of a clean up process is the removal of user accounts on a system previously created externally as a result of the penetration test. It is always the penetration tester's responsibility to inform the organization about the changes that exists in the system as a result of the penetration test and also to clean up this mess.

Limitations of Penetration Testing

There are many security problems for which penetration tests will not be able to identify. Penetration tests are generally carried out as "black box" exercises, where the penetration tester does not have complete information about the system being tested. A test may not identify a vulnerability that is obvious to anyone with access to internal information about the machine. A penetration test can only identify those problems that it is designed to look for. If a service is not tested then there will be no information about its security or insecurity. A penetration test is unlikely to provide information about new vulnerabilities, especially those discovered after the test is carried out.

Even if the penetration team did not manage to break into the organization this does not mean that they are secure. Penetration testing is not the best way to find all vulnerabilities. Vulnerability assessments that include careful diagnostic reviews of all servers and network devices will definitely identify more issues faster than a "black box" penetration test. Penetration tests are conducted in a limited time period. This means that it is a "snapshot" of a system or network's security. As such, testing is limited to known vulnerabilities and the current configuration of the network. Just because the penetration test was unsuccessful today does not mean a new weakness will not be posted on Bugtraq and exploited in the near future. Also it does not mean that if the testing team did not discover the any vulnerability in the organization's system, it does not mean that hackers or intruders will not.

Conclusions

It is important to make a distinction between penetration testing and network security assessments. A network security or vulnerability assessment may be useful to a degree, but do not always reflect the extent to which hackers will go to exploit a vulnerability. Penetration tests attempt to emulate a 'real world' attack to a certain degree. The penetration testers will generally compromise a system with vulnerabilities that they successfully exploited. If the penetration tester finds 5 holes in a system to get in this does not mean that hackers or external intruder will not be able to find 6 holes. Hackers and intruders need to find only one hole to exploit whereas penetration testers need to possibly find all if not as many as possible holes that exist. This is a daunting task as penetration tests are normally done in a certain time frame.

Finally, a penetration test alone provides no improvement in the security of a computer or network. Action to taken to address these vulnerabilities that is found as a result of conducting the penetration test.

Bibliography

Books:

[1] Joel Scambray, Stuart McClure, George Kurtz. “Hacking Exposed 2nd Edition” (2001).

[2] Ivan Arce, Maximiliano Caceres. Core Security Tecnologies. "Automatin Penetration Tests: A new challenge for the IS industry?" (2001)

[3] Stan Kiyota, Corporate Systems “Creating an Integrated Internal and E-Business Information Security Architecture” (2001)

[4] Reto E. Haeni. The George Washington University. Firewall Penetration Testing (1997)

Online Resources:

[5] Insecure. Fyodor's Exploit World, Exploits for many Operating Systems including Linux, Solaris, Microsoft, Macintosh. For Hackers, Hacking, Computer Security Auditing & Testing.
URL: http://www.insecure.org/sploits.html

[6] Pete Herzog. The Open Source Security Testing Methodology Manual
URL: http://uk.osstmm.org/osstmm.htm

[7] Wallyware, Inc. Hacker Whacker: See your computer the way hackers do
URL http://hackerwhacker.com/

[8] Lincoln d. Stein. The World Wide Web Security FAQ
URL: http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html

[9] Linet Solutions. Firewall TCP/UDP Ports: Which Protocols to Filter
URL: http://www.ec11.dial.pipex.com/port-filter.htm

[10] The Penetraiton Testing Group. An Introduction to Penetration Testing
URL http://www.penetration-testing-group.co.uk/index.htm

[11] Hideaway.net. Strategic Scanning and Assessment of Remote Hosts
URL: http://www.hideaway.net/Server_Security/Library/General/gentxts/ssarh.htm

Appendix A: Netcraft (www.netcraft.com) results on www.sans.org

The site www.sans.org is running **Apache** on **Linux**.

Samples of system uptime at www.sans.org

Note: Uptime - the time since last reboot is explained in the FAQ Latest data 30-Sep-2001

Display Options: Moving Average: 90 days Redisplay Graph

Uptime Summary for www.sans.org

Note: Uptime - the time since last reboot is explained in the FAQ Time in Days

Plotted Value	No. samples	Max	Latest
BSD/OS	172	123.22	12.49
Linux	37	75.91	75.91
90-day Moving average	310	33.85	26.22

OS, Web Server and Hosting History for www.sans.org

OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache	20-Sep-2001	12.33.247.6	ALTENET SOLUTIONS
Linux	Apache/1.3.20 (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b	16-Jul-2001	12.33.247.6	ALTENET SOLUTIONS
BSD/OS	Apache/1.3.9 (Unix) secured_by_Raven/1.4.2	23-Mar-2001	167.216.133.33	Digital Island, Inc.
BSD/OS	Apache/1.3.9 (Unix)	21-Mar-2001	167.216.133.33	Digital Island, Inc.
BSD/OS	Apache/1.3.9 (Unix) secured_by_Raven/1.4.2	1-Nov-2000		

167.216.133.33	Digital Island, Inc.

Appendix B: Penetration Test Tools

Some of the tools that are popularly used for penetration testing are shown in this appendix. The tools below are grouped according to the testing methodologies outlined earlier.

Information Gathering:

Nmap – Network scanning, port scanning and OS detection
URL: http://www.insecure.org/nmap/index.html

hping – Tool for port scanning.
URL: http://www.kyuzz.org/antirez/hping.html

netcat - Grabs service banners / versions.
URL: http://packetstorm.securify.com/UNIX/netcat/

firewalk - Determining firewall ACLs.
URL: http://www.packetfactory.net/Projects/Firewalk/

ethereal - Monitoring and logging return traffic from maps and scans.
URL: http://www.ethereal.com/

icmpquery - Determining target system time and netmask.
URL: http://packetstorm.securify.com/UNIX/scanners/icmpquery.c

strobe - Port scanning utility
URL: http://packetstorm.securify.com/UNIX/scanners/strobe-1.04.tgz

Vulnerability Detection:

Nessus - Scans for vulnerabilities.
URL: http://www.nessus.org/

SARA – Another scanner to scan for vulnerabilities.
URL: http://www.www-arc.com/sara/

Penetration Tools:

Brutus – Telnet, FTP and HTTP Password cracker
URL: http://www.hoobie.net/brutus

LC3 – Password cracking utility
URL: http://www.atstake.com/lc3