Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Instruments of the Information Security Trade

It would be a 'perfect world' if all of the computers today were secure. Unfortunately, somebody would want to look at something that they don't have access to. Penetration testing has many pros and cons, but many questions need to be answered before beginning. The most important piece throughout this entire penetration testing process is to know what you want to accomplish and then have a strategic plan in place that will provide step by step of what is expected to happen and have a contingency plan just in case. In c...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Instruments of the Information Security Trade

Mark Graff, November27, 2001

SANS Security Essentials GSEC Practical Assignment Version 1.2f(amended Aug.13/01)

Penetration Testing:

Internet security is extremely important today. The amount lost due to intrusions and hacking incidents has increased tremendously over the years. (1) How important is security to your company? Is your company at risk? How do you really know for sure? Periodic penetration testing can help you determine whether your company has the necessary controls in place to protect your organization. These tests will show how secure or how vulnerable your company's networks are to an attack and the results will open up the eyes of management as to what could happen to the companies assets. The results of these tests alone justify the importance of security within your organization. Penetration tests will also provide results of how your systems and employees react to an attack along with testing the current procedures that are in place. (6)

Although there are many benefits to penetration testing there are also many risks. Who should be running these tests? Do you want someone running penetration tests that would have full knowledge (example: current employee) about the environment or do you want someone with zero-knowledge (example: out-sourcing company) to run the tests? Zero knowledge attacks are performed by a penetration tester that has no knowledge or information about the environment they are attacking. These attacks provide the most realistic penetration attacks in that they would be performed to simulate a hacker in the outside world. The Full-knowledge attack that is performed by a penetration tester is familiar with the environment in detail. These attacks are designed for those attackers that have knowledge of the environment such as a previous employee. (2) What if the results are leaked? Imagine if a hacker or the media got hold of this information! Is there someone who understands and will act upon the results of the penetration tests? These are all risks of penetration testing and can be minimized by preparing properly and following the appropriate methodologies.

Methodology Tools Of the Trade:

The company's systems and networks need to be able to handle the penetration testing process. As mentioned earlier, the results from the tests will provide areas that continually need to be improved upon and will justify the importance of security within your organization. A strategic plan needs to determine the goals of the testing; where and how often the testing should be conducted; who will perform it; and the method for measuring, communicating and safeguarding the results. Information security practices today depends on sound policies, effective risk assessment, and properly constructed response procedures to security related incidents. It is very important to follow all of these practices. For instance, an information security policy should state who can conduct the penetration tests as well as who handles the results. Contingency plans need to be in place in case something unexpected were to happen which would help minimize the disruption of the environment. (3)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Test results must provide a good description and identify the exact machines in the network within your company that allowed the unauthorized access. Better results from your testing would include a detailed breakdown of percentages according to the test programs or scripts that were being used.

Test metrics should be developed. The information security world still depends on verbal description in most, if not all, phases of its activities. One of the many problems with verbal descriptions, however, is that they are not precise. The development of simple, straightforward metrics like the percentage of machines that crashed during a denial of service is very critical to the ability of the tests to achieve accurate, reliable results.

Upon completion of the penetration testing, the next important piece is to integrate the results of the tests in information security policies, standards and procedures. Finding out that a systems analyst had witnessed the attacks on networked machines, but did nothing about the attacks, would suggest that there should be changes to the company's security incident and response policies and procedures. When the changes have been made, the designated employees should systematically track them to ensure that they are being incorporated into everyday tasks. (4)

When strategic plans are not in place this is when the results from the penetration tests not communicated properly or inaccuracies and rumors take place. The proper strategy for managing the penetration testing process includes instructions for communicating the test results to management and to the key business members. The detailed penetration report most likely will not be the appropriate report for management due to its technical nature but several reports based upon different tests could be created for the separate audiences that the results should be presented to. (5)

Accountability and ownership should be established for the penetration testing process. The entire responsibility for the penetration test really is with the owner or the owners of the process. Within a huge company, many process owners may be appropriate but within a small company there may only be a single owner. Remember that an upper management show of support is usually required within a large company in order to have effective penetration testing and effective handling of results. The owners of the penetration tests can ensure that the company's business requirements are achieved through the testing process and are conducted properly. (5)

Lessons learned from the penetration tests should be shared confidentially. The professionals who completed the penetration tests should share this information confidentially within their own organization among those that require this information. The sharing of test information outside of the organization should include manager's approval and a completion of a non-disclosure agreement before any results are released. Also, do not post any questions or information to newsgroups or websites, which could reveal information about security exposures within your company. (2)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The company's information security training and awareness program should also benefit from the penetration testing. The training should not teach employees how to conduct penetration tests but it is important to train the company's system administrators, managers and sometimes even end users about testing restrictions, the precautions to take when interpreting results, and the appropriate responses for detection of an unauthorized test. (2)

Software Tools of the Trade:
Provided below are some free defense utilities or tools of the trade that will help you with your penetration testing.

Bastille – These are a collection of tools and scripts for "hardening" Red Hat Linux distributions once they are out of the box and best done before they are put into production. They aid new system administrators in making Red Hat more secure. Bastille Linux project – **http://www.bastille-linux.org/**

Crack – Crack is one of the original and still widely used password crackers for UNIX based systems. Used by white hats and black hats alike. Alec Muffett, Developer – **http://www.users.dircon.co.uk/~crypto/download/c50-faq.html**

Ipmasquerade – This is a Linux network address translation (NAT) function that is incorporated into most Linux distributions. Often Ipmasquerade is combined with Ipchains to form rule-based, routing and network access points. Information – **http://ipmasq.cjb.net/**

Linux FreeS/WAN – These services allow you to build secure tunnels and VPNS via IPSec/IKE implementation. Linux FreeS/WAN Project – **http://www.freeswan.org/download.html**

Nessus – This security scanner is intended to update and improve on SATAN. It is one of the many vulnerability-based scanners. The "Nessus" Project – **http://www.nessus.org/download.html**

NMAP Portscanner – This network port scanning tool can be utilized to scan networks for open ports and even OS identification. "fyodor" – **http://www.insecure.org/nmap/**

SAINT – This vulnerability-based security scanner, also has an available "WebSAINT" version. World Wide Digital Security Inc. – **http://wwdsilx.wwdsi.com/saint/**

Shadow – Intrusion detection system based on TCPdump, developed in part by the US Navy. Naval Surface Warfare Center – **http://www.nswc.navy.mil/ISSEC/CID/**

Squid – This is a full-featured Web proxy cache that supports Internet Caching Protocol (ICP) and SSL. Duane Wessels, project coordinator – **http://squid.nlanr.net**

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Sudo – "Superuser do" allows controlled access to root. This Unix based utility can be used to log superuser use and to restrict access to users or groups. Todd C. Miller, project coordinator – **http://www.courtesan.com/sudo/**

Tripwire – This commercial version of freeware Intrusion Detection System remains open source and holds some free capabilities. Tripwire Inc. **http://www.tripwire.com/downloads/**

Penetration Testing Tool Sites:

www.cotse.com - the computer professionals reference: **http://wetelephant.cotse.com/tools/**

Tips for NT Administrators in the area of Penetration Testing, Hacking, and Intrusion Detection: http://www.is-it-true.org/pt/#GlossP

Attack Techniques:

It is important that system administrators and network operations staff are informed of the risks and the threats to their business environment. Some attack techniques below are the favorites of hackers.

Password cracking tools have been part of a hacker's tool kit for a long time. The idea is for the hacker to initially steal the encrypted file from the victims' machine. The wide majority of systems, including Windows NT and UNIX, store the encrypted passwords in the file systems so that users can authenticate during login. Once the hacker has the encrypted password file he then places the file into a password-cracker that runs along side a dictionary word listing. The password-cracking tool tries to break the passwords by encrypting the entries in the dictionary and comparing it with the encrypting values of the password file. If the encrypted values match, the hacker will know the password. If the values do not match, the tool can continue by using a brute force attack method that goes through all combinations of characters. The only factor with this method is the amount of time a hacker has because with computers today getting faster and faster this process will only take a short time before the passwords will be broken. (7)

Organizations spend a lot of time and money implementing and maintaining firewalls so that that they can protect the company's networks from attack. The firewall is useless when the company allows unsecured modems to sit on the desks of their employees representing a side window so to speak for intruders. Attackers use war dialers for locating these modems allowing them to break into networks. They are among the intruders' favorite tools. A war dialer dials a listing of telephone numbers and tries to find a modem with a familiar carrier tone. Once the carrier tone has been found by the war dialer, the attacker is able to connect to those systems and attempt to login. (7)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Programs such as telnet, rsh, rlogin and FTP are all vulnerable to hijacking attacks. Any basic sniffer will give an attacker the clear text passwords when these protocols are in use. The problem is that any attacker who is connected to a network segment between the client and the server can use a session hijacking tool to take over a session. When a legitimate user is logged into a command line session, the hijacker can find the session take over for the user and reset the client connection. The hijacker then has complete control of that login; all subsequent accesses, changes and deletions will be recorded as the legitimate user's actions. The user will simply notice that the session has been dropped and assume that the network interrupted the communication link. (7)

Unix root exploits allow attackers with a user-level account on a UNIX system to gain Superuser access. Once they have achieved this access the attacker has the ability to hide his tracks by escalating their privileges on a UNIX system. New exploits are discovered weekly. (7)

Denial-of-Service (DoS) attacks purpose is to make a resource inoperative. These attacks target users, a host computer, or even a network that consists of operating systems, routers and even printers. The attacks can not only be a nuisance to organizations, but can also cost your company a significant amount of money in employee downtime, lost transactions or loss of investor and customer confidence. (7)

Conclusion

It would be a 'perfect world' if all of the computers today were secure. Unfortunately, somebody would want to look at something that they don't have access to. Penetration testing has many pros and cons, but many questions need to be answered before beginning. The most important piece throughout this entire penetration testing process is to know what you want to accomplish and then have a strategic plan in place that will provide step by step of what is expected to happen and have a contingency plan just in case. In conclusion, penetration testing if done properly, will benefit your organization.

References

(1) CSI. "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar". 12 March 2001. URL: **http://www/.gocsi.com/prelea_000321.htm**

(2) Kurtz, George and Chris Prosise. "Penetration Testing Exposed – Part 3 'Audits, Assessments & Tests (Oh, My)'". September 2000. Information Security Magazine. URL: **http://www.infosecuritymag.com/articles/september00/features3.shtml**

(3) CERT Coordination Center. "CERT System and Network Security Practices: June 6, 2001. "URL: **http://www.cert.org/archive/pdf/NCISSE_practices.pdf.**

(4) Piscitello, David. "Your First Penetration Test". WatchGuard LiveSecurity. URL: **http://www.corecom.com/external/livesecurity/pentest.html**

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

(5) Graham, Robert – FAQ: Network Intrusion Detection Systems. URL: **http://www.robertgraham.com/pubs/network-intrusion-detection.html**

(6) Winkler, Ira. "Penetration Testing Exposed – Part 1 'Audits, Assessments & Tests (Oh, My)'". July 2000. Information Security Magazine. URL: **http://www.infosecuritymag.com/articles/july00/features4.shtml**

(7) "Tool of the Trade". 1999. Information Security Magazine. URL: **http://www.infosecuritymag.com/articles/1999/toolsofthetrade.shtml**

© SANS Institute 2001, Author retains full rights

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**