GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Vulnerability Assessment
Susan Cima
July 6, 2001
Version 1.2e

I. OVERVIEW
II. DEFINITION
III. STATISTICS
IV. REPORTING
V. CLASSIFICATION
VI. PROTECTIVE MEASURES
VII. TOOLS
VIII. CONFIGURATION MANAGEMENT
IX. CONCLUSION
X. APPENDIX A
XI. REFERENCES

© SANS Institute 2000 - 2005, Author retains full rights.

I. Overview

The intention of this paper is to:

- Provide basic information to those who have recently entered the security field.
- Provide some insight as to why a vulnerability assessment is necessary.
- Provide an overview of the vulnerability assessment process from discovery to baseline standardization.
- Provide some assistance to those who want to perform a vulnerability assessment but do not know where to start.

II. Definition

As documented by SANS, "Vulnerabilities are the gateways by which threats are manifested" (1). In other words, a system compromise can occur through a weakness found in a system. A vulnerability assessment is a search for these weaknesses/exposures in order to apply a patch or fix to prevent a compromise.

How do these weaknesses occur? There are two points to consider:

- Many systems are shipped with: known and unknown security holes and bugs, and insecure default settings (passwords, etc.).
- Many vulnerabilities occur as a result of misconfigurations by system administrators.

Ways to counteract these conditions include:

1) creating and abiding by baseline security standards,
2) installing vendor patches (when appropriate),
3) vulnerability scanning,
4) subscribing to and abiding by security advisories,
5) implementing perimeter defenses, such as firewalls and router ACLs,
6) implementing intrusion detection systems and virus scanning software.

See also Section VI. Protective Measures.

III. Statistics

Not to anyone's surprise, recent figures from numerous organizations, including CERT and CSI show a rise in intrusion attempts and attacks.

For instance, per the "2000 Computer Security Journal/FBI Computer Crime and Security Survey" (2), the trends that have emerged over the previous years are:

- Organizations are under cyber attack from both inside and outside of their electronic

© SANS Institute 2000 - 2005 Author retains full rights.

perimeters.
- A wide range of cyber attacks have been detected.
- Cyber attacks can result in serious financial losses.
- Defending successfully against such attacks requires more than just the use of information security technology.

Per CERT/CC statistics (3), the number of reported incidents went from 9,859 in 1999 to 21,756 in 2000. The number of vulnerabilities reported went from 417 in 1999 to 1090 in 2000. See http://www.cert.org/stats/cert_stats.html for more information.

What has been done in response to this increase in malicious activity?

- Vendor responses with more patches/updates.
- An attempt to increase public awareness of security issues by such organizations as CERT, SANS, FIRST, etc.
- The FBI has established the National Infrastructures Protection Center (NIPC) http://www.nipc.gov/ (possibly being replaced later this year with a new CyberSecurity Board commissioned by President Bush (4)) and the Regional Computer Intrusion Squads.
- The Department of Justice created the Computer Crime and Intellectual Property Section (CCIPS) http://www.cybercrime.gov
- New laws and regulations.
- Media attention.
- More tools in the security arsenal.
- Proposed stiffer penalties and jail time for those convicted.
- More responsibilities given to security professionals.
- See http://www.officer.com/special_ops/c_crimes.htm and http://www.computer-investigators.com/lawenforcement.html for more information on computer crime units.

IV. Reporting

Depending on who discovers the vulnerability, it can either be exploited or reported. Vulnerabilities are reported in the hope that the vendor will provide a timely patch or someone will develop a fix.

The following represents two avenues for reporting vulnerabilities:

- BugTraq's (a moderated mailing list specific to discussion of security vulnerabilities) vulnerability reporting protocol (5) is as follows:

    1. Contact the product's vendor and give them one week to respond. If they don't respond, post to the BugTraq list. See http://www.securityfocus.com for posting information.

© SANS Institute 2000 - 2005 Author retains full rights.

2. If you do hear from the vendor, give them what you consider appropriate time to fix the vulnerability. This will depend on the vulnerability and the product.

- CERT Coordination Center. CERT/CC's reporting form (6) can be found at http://www.cert.org/reporting/vulnerability_form.txt

There is some disagreement on the proper vulnerability reporting protocol. First, BugTraq publishes the exploit scripts. But other organizations, such as CERT, FIRST, and NIPC publish vulnerabilities without the exploit scripts. Each has their reasons for doing so. The difference in opinion is due to the fact that many attackers exploit the newly published vulnerabilities. Second, a person should act responsibly after discovering a vulnerability. Before releasing the problem to the public, they should give the vendor ample time to provide a patch. Releasing the problem to the public too soon can cause an increase in malicious behavior.

In light of this difference of opinion, committees have been formed by security-industry leaders to standardize security practices. One event, held in November 2000, was the Security Vulnerability Summit (7), a gathering of thirty industry leaders "to identify and discuss the principal issues surrounding security vulnerability disclosures". The goal of the Summit was to "create a clear, timely, and predictable process by which customers, vendors, government organizations and other key parties can be alerted to potential security threats and take the appropriate measures to protect their digital assets". See Appendix A for a follow-up to the Security Vulnerability Summit meeting. Also, you can read more at http://www.zdnet.com/enterprise/stories/main/0,10228,2652346-4,00.html.

However, creating an industry-wide standard is an overwhelming task and this is clearly a topic that needs further discussion.

V. Classification

Another problem facing the security industry is the way vulnerabilities are named or grouped. With various security professionals and product manufacturers giving different names to the same vulnerabilities, it can be confusing to the security practitioners who work in the field.

However, organizations have stepped in to help in developing a common language for the vulnerabilities. The result is CVE - Common Vulnerabilities and Exposures List (8). Sponsored by the Mitre Corporation, CVE has set a standard in the naming convention of security vulnerabilities making them easier to discuss & document. The entire CVE List of vulnerability naming standards can be downloaded at http://cve.mitre.org/cve/index.html.

Per Laura Taylor, founder of Relevant Technologies, the CVE "makes it easier for security vendors to develop intrusion detection and scanning tools. As more IT decision makers understand the meaning of CVE, products with CVE-compatible names will likely receive a better reception on the market".

Many products already use the CVE standard. They include:

- STAT (Security Threat Avoidance

© SANS Institute 2000 - 2005 Author retains full rights.

Technology) Scanner by Harris Corp. http://www.statonline.com/index.asp
- Internet Scanner by ISS Internet Security Systems http://www.iss.net
- Nessus Security Scanner http://www.nessus.org/

See http://www.cve.mitre.org/compatible/ for more CVE-compatible products.

VI. Protective Measures

Common exploits occur because of weaknesses found in a computing environment. These exploits are an attack against:

1. **Confidentiality** - being secure from unauthorized access. Example: Vulnerabilities in telnet (user names and passwords sent unencrypted from a remote connection) can allow an attack against Confidentiality.

2. **Integrity** - accuracy and completeness of data. Example: Vulnerabilities in sendmail (mail can be forged from any address) can allow an attack against integrity.

3. **Availability -** data and systems ready for use at all times by authorized users. Example: Variations in ping (request for information, can cause a denial of service attack - i.e., floods, ping of death) can be an attack against Availability.

Examples of Protective Security Measures

- access controls - user IDs and passwords, appropriate password and security policies,
- separation of duties,
- user authentication, with appropriate use of controls, where possible, e.g. smart cards, biometrics, etc.
- workstation lock screens,
- encryption,
- proper registry permissions,
- proper directory and file permissions,
- properly defined user rights,
- social engineering prevention,
- applying patches/updates,
- firewalls,
- VPN tunneling,
- screening routers,
- anti-virus software,
- prompt removal of terminated/transferred employee accounts, default passwords and unnecessary services running on the system,
- implementing and enforcing change control policy to limit activity to authorized users only,
- review and management signoffs of user authorizations,
- use of checksums with attendant software to report file modifications,

© SANS Institute 2000 - 2005 Author retains full rights.

- enable audit logging and perform log reviews,
- review of open ports and services,
- properly configured routers,
- searching for and disconnecting unauthorized or poorly configured modem services.

Vulnerability Listings

Various organizations maintain a vulnerability listing. They include vendor sites, such as, ISS http://xforce.iss.net/security_library/ and Microsoft http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/current.asp , and security organizations, such as SANS http://www.sans.org/topten.htm and CERT http://www.cert.org/current/current_activity.html

Tripwire has created a poster of exploits you can obtain at: http://www.tripwire.com/literature/poster/index.cfml?cfid=643809&cftoken=708

Subscribing to these site's newsletters will keep you abreast of current activity.

VII. Tools

There are different types of vulnerability scanners available: layer of analysis: host scanners, network scanners, database scanners; engine types and platforms; wardialers; open-source and commercial scanners.

What are the differences?
As stated in "FDIC: Risk Assessment Tools and Practices for Information System Security" (9),

Host based tools search for vulnerabilities on an individual computer.."are effective at identifying security risks that result from internal misuse or hackers using a computer system….detect holes that would allow unauthorized access…and confirm that various security policies are being followed".

Network based scanners "reside on the network to detect if it is vulnerable to known attacks….effective at detecting network attacks…can detect unauthorized systems on a network or insecure connections to business partners".

Database Scanners identify potential security exposures in database systems.

Wardialers search for modems, which are capable of providing unauthorized remote access to an organization.

Below is a sample of tools (10 - websites updated 7/16/01) categorized by their scanning platform - whether host, network, database-based or a wardialer.

© SANS Institute 2000 - 2005 Author retains full rights.

NETWORK BASED SCANNING TOOLS

NAME	ENGINE TYPE	OPENSOURCE	COMMERCIAL	WEBSITE
Cisco Secure Scanner	NT		X	Http://www.cisco.com/warp/public/cc/pd/sqsw/nesn/
Whisker	Linux	X		http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2
Retina	NT/2000		X	http://www.eeye.com/html/Products/Retina/
Nessus	Unix/Linux	X		http://www.nessus.com
Nmap Footprinting tool	Unix/NT	X		http://www.insecure.org/nmap/

HOST BASED SCANNING TOOLS

NAME	ENGINE TYPE	FREEWARE	COMMERCIAL	WEBSITE
STAT	NT		X	http://www.statonline.com/index.asp
CyberCop	Win32/Linux		X	http://www.pgp.com/products/cybercop-scanner/default.asp

© SANS Institute 2000 - 2005 Author retains full rights.

TARA	Linux/Unix	X		http://www.www-arc.com/tara/index.shtml
ISS System Scanner	NT/2000		X	http://www.iss.net/securing_e-business/security_products/security_assessment/system_scanner/
VigilEnt	Various		X	http://www.pentasafe.com/products/

DATABASE SCANNING TOOLS

NAME	ENGINE TYPE	FREEWARE	COMMERCIAL	WEBSITE
ISS Database Scanner	Oracle, SQL, Sybase		X	http://www.iss.net/securing_e-business/security_products/security_assessment/database_scanner/index.php
SQLdict	MS SQL	X		http://www.ntsecurity.nu/toolbox/sqldict/
Various Products for security of Databases	Oracle, SQL		X	http://www.pentasafe.com/products/vamsqlserver.htm

© SANS Institute 2000 - 2005 Author retains full rights.

WARDIALERS

NAME	FREEWARE	COMMERCIAL	WEBSITE
PhoneSweep		X	http://www.sandstorm.net/phonesweep/
Telesweep Secure Scanner		X	http://telesweepsecure.securelogix.com
ppp Scanner		X	Http://xforce.iss.net/static/804.php
THC Scan	X		http://www.thehackerschoice.com/
Modem Scan		X	http://verttex.com

Method

A general approach to vulnerability assessment would be roughly as follows: (Written authorization to perform these steps should be obtained from upper management.)

External:

- Use tools e.g. Nmap, Samspade, etc. to glean as much information about the target system as possible.
- Wardial all phone numbers and attempt penetration if targets are found.
- Try gleaning some useful information via "social engineering".
- If you can get the operating system ID from Nmap, use it to set up the scanner for custom probings.
- Update scanners with the latest attack signatures prior to use.
- Perform scans against all targets found.
- Analyze results and take corrective action.

Internal:

- Update scanner with latest attack signatures prior to use.

© SANS Institute 2000 - 2005 Author retains full rights.

- You may wish to do custom scans on selected machines that require simpler probe configurations, e.g., scan all system administrator and technical personnel machines for backdoors or other illicit software. You may be scanning all new servers prior to rollout for certification.
- Check for weak passwords using a password cracking tool.
- Analyze results and take corrective action.

Vulnerability Mapping

Another method that can be used to locate weaknesses within a system is called vulnerability mapping (11). This entails analyzing the software and services running on the computer, then matching each to a known vulnerability. Services can easily be found using a tool such as Nmap, DumpSec (http://www.systemtools.com/free_frame.htm) or Hyena http://www.systemtools.com/index.html . As mentioned previously, vulnerability listings can be found at CERT and BugTraq. If a vulnerability associated with a service running on the computer is found, the appropriate patch or fix should be applied. See CERT Report on "Identifying data that characterize systems and aid in detecting signs of suspicious behavior" at http://www.cert.org/security-improvement/practices/p091.html .

The guidelines suggested by CERT (http://www.cert.org/security-improvement/) will also help harden your system configuration and operational environment and protect it against known attacks. It covers planning, configuration, maintenance, improving user awareness, and testing.

Also, see http://www.anti-online.com/focus/ih/articles/vulnassess.html for a Vulnerability Assessment Survey developed by Richard Wiens.

VIII. Configuration Management

Configuration Management is the process of controlling changes made to a system's configuration after installation. Periodic reviews should be performed to ensure parameter settings are set as originally intended and not changed over the course of new installations and network updates.

Per Dr. Bruce Hartley in "The Process of Security" (12), "the best type of configuration management system involves defining a system for documentation, establishing a defined procedure for making changes to that system, and evaluating all changes against the overall security of the system and documenting them. You should also make sure you receive, evaluate and disseminate security warnings and advisories".

See specific CERT guidelines at http://www.cert.org/security-improvement/ and http://www.cert.org/nav/index_green.html

IX. Conclusion

Statistics show that system compromises are on the rise so we must guard against them using the methods available to us. Vulnerability scanners

© SANS Institute 2000 - 2005 Author retains full rights.

are one tool available for ensuring secure systems. However, scanners should not be the only weapon in the security arsenal. They should be used in addition to firewalls, intrusion detection tools, good security policies, and all the other defenses noted in this paper. Ideally, scanners should be used as a last defense to complement the security practices already in place. Just keep in mind that a good follow-up plan to correct any vulnerabilities found is just as important as detecting them.

X. APPENDIX A: Security Vulnerability Summit Outcomes (7)

Summit working groups

Unlike political "summit meetings" that plan their conclusions in advance, the Vulnerability Summit didn't end with a planned communiqué. Rather, it marked the beginning of a process in which working groups (most with three or more participants) will develop the issues and draft proposed statements of best practices. Following are the working groups formed at the summit and their missions.

Charter Definition Propose follow-on communication plan and threat- ranking system to make summit conclusions useful for continuing guidance to Web administrators and the general Web community.

Stakeholder Recognition Propose a means of resolving the gap between those who want maximum information at the earliest opportunity and those who prefer that threats not be widely disclosed before remedies are identified and available. Develop usable guidelines for distinguishing among intruders, authorized investigators and independent researchers.

Information Release Consider criteria and methods for publication of threat effects, preventive measures and technical details; evaluate role of press and opportunities for affirmative outreach/education of mainstream media outlets; coordinate with working groups on vendor notification and public relations.

Vulnerability Life Cycle Consider relative importance of immediate response to new threats vs. long-term knowledge-base maintenance as resource for system administrators; examine actual damage caused vs. age of threat.

Vendor Notification Propose guidelines for interaction between independent researchers, paid

© SANS Institute 2000 - 2005 Author retains full rights.

consultants, and vendors of vulnerable products or services; consider merits of vendor premium-support plans vs. full-scale disclosure policies as means of disclosing information and providing follow-up support to affected customers; coordinate with working groups on information release and public relations.

Vulnerability Verification Examine role and magnitude of hoaxes as burden on threat analysis; propose guidelines for vendors to invite/investigate vulnerability reports; weigh benefits of anonymous reporting (to encourage early discovery) vs. attribution requirements (to discourage irresponsible or malicious input).

Patch and Solution Development Propose criteria for disseminating workarounds, patches or remedies incorporated into general product upgrades, considering costs and secondary threats involved in testing/releasing/deploying/supporting updates in the field.

Public Relations Examine issues of credit for independent researchers, whose reputations are enhanced by role in threat discovery, vs. need to give vendors time to analyze threats before system attackers exploit them en masse; coordinate with working groups on information release and vendor notification.

Legal Issues Examine gaps between best-practice consensus vs. laws, licenses and international agreements. Consider issues of intent in determining criminality; consider role of proposed cyber-crime laws in providing false sense of security to users; consider spillover effects of cyber-crime laws in preventing legitimate investigation of vulnerabilities.

Ethics Propose statements of good-faith conduct for identified stakeholders.

XI. References:

(1) SANS GIAC Security Essentials Training Manual

(2) 2000 CSI Computer Security Journal

(3) CERT Coordination Center Statistics 1988-2001
http://www.cert.org/stats/cert_stats.html (last accessed 7/16/01)

(4) Verton, Dan. "Bush Said To Be Planning Cybersecurity Board" Computerworld Security Knowledge Center July 12, 2001.
http://www.computerworld.com/itresources/rcstory/0,4167,key73_sto62106,00.html (last accessed 7/16/01)

(5) BugTraq: FAQ http://www.securityfocus.com/frames/?content=/forums/bugtraq/faq.html (last accessed 7/16/01)

(6) CERT/CC Product Vulnerability Reporting Form v1.0
http://www.cert.org/reporting/vulnerability_form.txt (last accessed 7/16/01)

(7) Security Vulnerability Summit - http://www.vulnerabilitysummit.com/ (last accessed 7/16/01)

Rapoza, Jim. "Security Core: Best Practices". November 13,00. eWeek.
http://www.zdnet.com/enterprise/stories/main/0,10228,2652346-1,00.html (last accessed 7/16/01)

(8) Taylor, Laura. "A Common Language

© SANS Institute 2000 - 2005 Author retains full rights.

for Security Vulnerabilities" May 24, 01
Zdnet Business and Technology (last accessed 7/16/01)
http://www.zdnet.com/enterprise/stories/main/0,10228,2765107,00.html

Berg, Al. "Part 2: Audits, Assessments & Test (Oh My)". Information Security Magazine August 2000.

Common Vulnerability and Exposures http://cve.mitre.org/news (last accessed 7/16/01)

(9) FDIC. Financial Institution Letters "Risk Assessment Tools and Practices for Information System Security". http://www.fdic.gov/news/news/financial/1999/FIL9968a.HTML (last accessed 7/16/01)

(10) Talisker's Network Security Tools http://networkintrusion.co.uk/n_scan.htm (last accessed 7/16/01)

(11) Kurtz, George & Prosise, Chris. "Part 3: Penetration Testing Exposed". Information Security Magazine May 9, 2000

(12) Hartley, Dr. Bruce. "The Process of Security" Business Security Advisor July/August 2001

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: April 24th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor