

Vulnerability Assessment Survey

Richard Wiens 2000-09-29

Introduction

Organizations have a tremendous opportunity to use information technologies to increase their productivity. Securing information and communications systems will be a necessary factor in taking advantage of all this increased connectivity, speed and information. However, no security measure will guarantee a risk free environment in which to operate. In fact, many organizations will need to provide easier access by users to portions of their information systems, thereby increasing potential exposure.

Administrative error, for example, is a primary cause of vulnerabilities that can be exploited by a novice hacker, whether an outsider or insider in the organization. Routine use of vulnerability assessment tools along with immediate response to problems identified will alleviate this risk. It follows, therefore, that routine vulnerability assessment should be a standard element of every organization's security policy.

This Vulnerability Assessment Survey has been designed to allow organizations to build up their crisis management capability. Its purpose is to help answer the question: "How secure is your organization's information?" This crucial question emerges over and over as one of the highest priorities in an organization.

The Survey allows the organization to develop their crisis planning capability by:

- Detailing the vulnerabilities of the organization
- Developing response plans and procedures
- Improving capability of crisis management teams

Assessment Strategies

In the ideal world, the assessment strategy begins before a computer network becomes operational with the individual computers so that no flawed computers are introduced into the network. The network can then be probed for security vulnerabilities. Finally, the external network defense, the firewall, is verified before any connection to a public network is allowed.

In reality, there are often existing computer networks and external Internet connections. This situation introduces a significant number of known vulnerabilities. The tendency is to squander scarce resources on the most prominent vulnerabilities rather than investing the effort on the vulnerabilities that pose the greatest risk to the enterprise.

VULNERABILITY ASSESSMENT SURVEY

Company:

System:

Address:

Point of Contact:

Office Symbol:

Phone Number:

Email Address:

(NOTE: THIS CAVEAT APPLIES TO EACH OF THE FOLLOWING QUESTIONS. "GET PROOF OR FURTHER EXPLANATION WHEN REQUIRED.")

IMPORTANT REMINDER: Tour the facility first!

Hardware

What does the network infrastructure look like? Is a diagram available? If not, what does it look like? (Get a detailed description/depiction.)

What is the network topology?

What kinds of cables are used?

What are all the data outlets?

What type, how many, and where are any servers?

What type, how many, and where are any workstations?

What type, how many, and where are any printers?

What type, how many, and where are any modems?

What type, how many, and where are any network (LAN/WAN) connections?

Do any of these connections have a security device on them?

Is there any cable management, to include: security, and auditing?

Are there routers or gateways on the network? If so, what kind, how many, and where?

Are there concentrators, switches, bridges, or hubs? If so, what kind, how many, and where?

Are there any firewalls? (software and hardware?)

Are any proxies used by the system?

What is the location and type of all and any hardware that was not addressed?

Is everything turned on? Is anything unhooked, separate, or off?

Is the router configuration default?

Are there any router security implications? Position of the router on the net? Default configuration?

Does the system support perimeter router filtering?

Are there perimeter router filtering policies?

Are there perimeter router rules? If so, what are they?

Does the system support Cisco IOS router configuration commands?

Does any part of the system filter packets?

Is there a packet filtering policy?

Are there any installation standards? If so, what are they? (Do they meet the regulations?)

Are there any intelligent external devices?

Physical Security

Is there any physical security? For example, is there fire detection/suppression equipment in place or planned? Has visibility related to the equipment been reduced, and/or has access to the equipment or area been limited?

Is there any equipment that is physically not secure?

Is the system IAW DA physical security requirements?

Are there a restrictions on the boot process? Servers and workstations? Only root should be able to reboot?

Is there a password on the CMOS/BIOS?

Are there procedures for logging off or locking the server/workstation?

Are the default user screensaver options configurable and or used?

Is the hardware vulnerable to theft?

Is there opportunity for unauthorized access or use?

Does the system have any drives (floppy, CD, etc) that could be accessed by the public?

Contingency Plans

Is there a contingency plan?

Is the system prepared for losing power? i.e. is the information backed up?

Is there an UPS, generator, or back-up power?

Are approved personnel designated in the system back-up and recovery process?

Is there protection for power surges or voltage spikes?

Environmental & HVAC

Are there any environmental concerns that may affect the system?

Are there any HVAC issues that may affect operations?

Configuration Management

Is the configuration approved (C2/ AR 380-19) for the level of sensitivity (SBU)?

Is there any configuration management in place? Is it written?

Is there a configuration manager (CM) established?

Does the CM control all connections to other systems?

Does the CM control all system documentation?

Are there system rules of behavior? What are they? Are they written?

Is there a formal or Informal review of architecture modifications for security impact?

Does the system have a method for controlling what patches are applied to the system?

Is there any software configuration management? (Licenses, patch control, version control)

Communications

Is there LAN or WAN connectivity?

Is there Internet connectivity?

Are there modems on the system? How many and where? Are they RADIUS compliant? Waivered? Credit Card modems?

Have all types of data been considered, e.g., backups, archived data, metadata, parameters, control data, and derived data?

Is it clear that the availability and confidentiality of the system requires that communications be maintained error-free and available on demand 24 hours a day, seven days a week, 365 days a year?

Does the system require that information pass only to properly authorized personnel for appropriate use?

How are the modem settings configured?

Is it possible that a poorly configured dial-up connection exists so that an intruder can gain access to the system?

Are callback procedures used for modems?

Is there a method to account for the use of IP or IPX addresses?

Is encryption being used for anything? If so, what?

Is information sent in the clear over the system?

Is information sent in the clear across the Internet?

Is the integrity of the data assured during transmission? If so, how?

Is the confidentiality of the information assured during transmission? If so, how?

Are there means by which non-repudiation is effected?

Is there sensitive information sent over the network? (Privacy Act?)

What protocols are available on the network? Which ones are used? For what purpose? (TCP/IPX/SPX)

Network Level Protocols

What network services are available on the servers? (Telnet, FTP, TFTP, SNMP)

Is the system accessed by phone numbers in any way? Can the system access other phone numbers in any way?

Does the system use leased/dedicated lines? (Paragain, T1, Copper)

Does the system have communications servers? What for, where, with what services?

How is the communications server accessed? By who?

Are there procedures for communications server management? What are they and who does it?

Does the system have any multiplexers? What are their functions? Where are they? How are they accessed?

Are any steps taken to secure the multiplexers?

Does the system have any phone line connections? Where and why?

Do any of the system components permit remote configuration?

How are (if any) components remotely configured?

What is the bandwidth of your connection to you service provider? How much of that do you use? What do think your bandwidth requirements are?

Recovery and Incident Handling

Are there procedures to identify and respond to security events?

Are there procedures for the Identification, notification, and response to suspected attacks?

Are there procedures for the containment of security concerns?

Are there procedures for the eradication of specific security concerns?

Is there virus protection on the system?

How is the virus software configured?

What version or latest update is being used?

Are there procedures in place for vulnerability identification and correction?

Does the system maintain logs or audit files?

Are there methods in place to ensure the preservation of logs?

Are there procedures in place to effect the recovery of the system?

Are there methods for file recovery on the system?

Are there any network intrusion detectors (NID) on the system?

In what fashion is the NID Used?

What does the NID do in terms of protection?

What are the NID detection rules?

Software

What applications are on the system? What are their functions?

Are the applications in their default configuration? With default accounts and security posture?

Is there any contract maintenance? If so, by who, for what, and how?

Is there any remote administration on the system? If so, by who, for what, and how?

What access control is on the system? (Network/Applications/OS/email logins)

How are the permissions configured? (Applications) Can users access more than they need?

What application specific ports are open/in use? Are any ports blocked?

Can the general user install programs?

Are backup copies of software maintained?

Are software modifications controlled or monitored? (Patch or upgrade)

Are licenses audited?

Can users exit the applications to gain access to the operating system?

Are applications and software protected by passwords?

Do help desk personnel have access to anything on the system? If so, who are they, do they have access to the system, and how?

Does the system have maintenance accounts?

Are there group accounts on the system?

Does the system have any default accounts?

Does the system have any unused accounts?

Does the system have remote administration capability?

Does the system have diagnostic ports?

What tools are available to the user on the system? (bin, sbin)

Are administrator tools available? NTRK/Admintool/On-Site, roots path (bin)(sys)?

How available are they? Can users access them?

Media Security

Does the system process Sensitive But Unclassified (SBU) information?

Does the system accommodate floppy disks, removable drives, zip drives, etc?

Is the system output protected? The monitor/screen, floppies, HD, printer?

Are there means by which output is tracked?

Is the media marked in a manner that would identify it as containing SBU?

Are there means by which media is sanitized?

Are passwords contained on any of the media? If so, what, where, how, why, and is it protected?

Does any of the media contain SBU?

Is any of the SBU media disposed of or reused? How so?

Are there any procedures for the disposal of media? If so, what are they?

Is media sanitized before disposal?

Are the methods of disposal approved?

Are the methods of disposal controlled?

Integrity

Are there methods in place to ensure and check hardware integrity?

Are there methods in place to ensure and check software integrity?

Does the system employ any free software?

Are there methods in place to ensure and check the integrity of system files and stored information?

Are there methods in place to ensure the confidentiality of the information on the system?

Are there methods in place to ensure and check file location on the system?

Are the files backed up on the system?

Are there methods in place to ensure log integrity?

Personnel Security

Do any users on the system have an ADP Level? If so, who at what level, and why?

Are the users on the system locked into their specific area that they need to operate? Can they access things that they do not need to know?

Do any foreign national personnel have access to the system? What is their position and level of access?

Are there methods and procedures in place for personnel password management?

What is the process for account creation and deletion? Do users have access to that process?

Does the system adhere to a set of general standards concerning personnel (system rules of behavior)? If so, what are they?

Are adequate user authentication mechanisms (such as firewalls, dial-in controls, Secure ID) in place to limit access to personnel?

Are background or reference checks used for individuals who have routine access to sensitive information?

Are individuals in sensitive positions subject to job rotation so that there is as much separation

of sensitive job functions as possible?

Are there clear policy statements and controls concerning the intent of the organization to protect the data resources from accidental or deliberate unauthorized disclosure, modification, or destruction.

Administrative Security

Do you attempt to comply with the applicable regulations? 25-IA, AR 380-19, 5200-28? Do you have them?

Does the system have any of the applicable written policies? (Password, marking, auditing, access, etc)

Security Awareness Training

Is security awareness training in place?

Is the training scheduled regularly? With what frequency?

Does the training require mandatory attendance?

What items are covered in the training?

Have the staff personnel been fully briefed on how to mitigate system security risk?

Computer Security

Does anything on the system use identification and authentication in the clear across the network or Internet?

Does the system have operations guidelines? (hours, location, and type of work; user access and login privileges restricted to duty hours?)

Is there an inactivity timeout on the system? Logout/Screensaver?

Does the system require passwords to gain access?

What are the password rules or guidance?

Where is the password file kept?

Are there any backdoor circuits on the system (connections to anything other than the connection to the indigenous system)?

If there is SBU on the system, are the passwords randomly generated?

Is the password file protected? How?

Does the system run a time synchronization process to keep the workstations in sync with the server?

Does the system permit NetBios access from the Internet?

Does the system use dynamic host configuration protocol?

Does the system use the DISA information assurance vulnerability alert (IAVA) process?

Wide Area Connectivity

Can the system be remotely accessed?

Does remote access require user id and password?

Does the system use warning banners?

What info is offered by login banners? Normal login, telnet and ftp logins?

How is the router accessed? By whom and why?

Does the system employ access control lists? How are they configured?

Is router change management in place? By whom and how?

Does the system have its own domain name service?

Are there procedures for network address management?

Does the system employ Network Address Translation? (Firewall IP change to hide internal IP's)

Are there any virtual private networks (VPNs) on the system? (Get a description.)

Are there any virtual local area networks (VLANs) on the system? (Get a description.)

Are any routers leased and maintained under a maintenance contract?

Are any routers running config stored on a TFTP Server? If so, can the router config can be read and written to?

Are there any dual-homed servers or workstations? (i.e., computers with 2 NIC cards with access to 2 subnets at once.?) If so, is IP forwarding enabled?

Are any servers acting as mail servers? (i.e., Exchange)

Network Management

Is there a central network management station?

Common Attacks

Can users exit the application? (Ctrl Alt Delete, F keys, Hot keys, Ctrl C, etc)

Can users access the CMOS on the server or their work station? Are the CMOS's password protected?

Is system prone to log access and doctoring by users?

Has the system ever been checked for malicious code or hacker tools?

Operating Systems Windows NT

Does the system accommodate DOS compatibility files?

Securing the Registry

Has the option to save the password in the dial-up networking function been disabled?

Are procedures in effect to delete cached roaming profiles?

Are procedures in effect to restrict access by NULL sessions?

Does the system display a legal notice for FTP server service?

Account Policies and User Rights

Is the system currently set to audit? To what extent? (Appendix ? of the NT STIG)

Does system have audit log requirements for workstations?

How, if at all, are the logs protected?

Are system administrator actions logged?

Does the system support Windows NT Remote Shell Service (RSH)? Is it running? Why and how?

Is Windows NT schedule service running on the system?

Do applications on they system have any security features?

Is the system running Microsoft Systems Management Server (SMS)?

Disaster Recovery

Is there an emergency repair disk (ERD)? Where is it stored?

Novell Netware

Does the system have NetWare Client software running?

Is the system running NetWare server software?

NDS Security

Does the system employ identification and authentication methods?

Are administrator, user, or groups verified and documented by the ISSO?

Is the Netware server console locked with a unique password?

UNIX

Does the system employ user account controls? How?

Are there any inactive accounts on the system?

How do users access their account?

What password controls are on the system?

What password guidelines are adhered to?

Is there any special privilege access on the system?

Who has access to the root account or other high level accounts on they system?

How is the root account accessed? Remotely? Encrypted?

Are group accounts used on the system?

Are resources controlled on the system? How? (Kernel, drives, printers)

How are the permissions set? (minimal rights?)

Do users have home directories?

Can users exit the application and access a shell?

Network Services

Is Rlogin or Remote Shell (rsh) running?

Is Rexec running?

Is the Finger port open?

Does the system accommodate remote host printing?

Is Sendmail or the equivalent running on the system? What version?

Is Trivial File Transfer Protocol (tftp)?

Is X Windows on the system at all? Is it running?

Is UNIX-to-UNIX Copy Program (uucp) running?

Is HoneyDanBer on the system?

Does the systems have hosts files?

Does the system use symbolic links?

Does the system have .rhosts or hosts.equiv files?

Is the System Logging Daemon (syslogd) running on the system?

Is Secure Shell (ssh) running on the system?

Trust Relationships

Is the system using Network Information Service (NIS)?

Is the system using Network Information Service Plus (NIS+)?

Is the system using Network File System (NFS)?

Are any UNIX Security Tools being used on the system?

Vulnerability assessment tools:

- Enterprise Security Manager (ESM)
- Computer Oracle and Password System (COPS)
- Security Profile Inspector (SPI-NET)
- CRACK
- Tripwire
- Intruder Alert (ITA)
- Ifstatus and Cpm
- Wrapper programs
- Sendmail Wrapper Program
- TCP_Wrappers

Web Servers

Is the web server administration centralized? Who is it? Where is it?

Who owns the server hosting the web-site?

Is the server on the Internet or intranet?

Is it publicly accessible?

Is access to the server controlled? (Is remote access possible?) (Is there a strong I&A prompt in place in order to login at the console?)

Does the system specify users and groups?

Are restrictions defined by Internet Protocol (IP) address?

What web server software is used?

How is the web server security configured? (entire profile)

How are the web server preferences configured? (entire profile)

What is the server platform?

Is it secured by any means?

What web application ports are open/running?

Are there user and administrative accounts for the web-site?

Does the web server maintain logs? If so, what?

Does the web-server also perform e-mail server functions?

Does it run Telnet? Why?

Does it run File Transfer Protocol (FTP)? Why?

Is there any web server application security? (web-site login or SSL, etc.)

Are any scripts used?

Is Active X used?

Can Improper Input run: cookie or tag; longer than variable input; non-alphanumeric; values outside defined scope?

Are any Perl Scripts used? (They may not include the current directory) Has taint been activated?

Is JavaScript used?

Are Java applications used?

Is a Java verifier used?

Is a Java Class loader used?

Is private/public key infrastructure used?

Is Secure Socket Layer (SSL) used?

Does the system make use of certificates to control server access?

What are the server configuration details?

Are any firewalls or proxies employed?

Web Client Security

Does the client have virus protection?

What client browsers are used?

Is there a policy for the configuration of the browsers?

Are the general preferences defined for the user?

Are the security preferences configured by the SA? If so, how are they configured?

Are any scripts used?

Are any personal certificates used?

Is there any security software on the system?

Are passwords used?

Email Servers

What operating system is it running?

What email program is used?

Is the email server administration centralized? Who and where?

Is it used to process email on the intranet, Internet, or both?

Who can access the server and how?

Is SBU or Privacy Act info sent via email over / on the system?

Does it specify users and groups? How?

How is the mail server security configured?

Is there any mail application security?

What is the server hardware?

Is it secured by any means?

How are the directories and file protection configured?

How are file and directory access rights configured?

What mail application ports are open and running? (POP3, NNTP, SMTP, LDAP, IMAP4)

Are there user and admin accounts?

Does the mail server maintain logs? To what extent?

Can you access email via the Internet? How? Does it require login and password?

Is there virus protection to check email?

Is mail automatically routed to the client or is it read from the server?

Are any scripts used?

Does it accept anything other than text in the email body?

Is there any content blocking? (.exe attachments, etc?)

Does the system employ PKI?

Does the system use SSL?

Are any firewalls, proxies, or remailers used?

Does the system permit anonymous remailing?

Will the system accept anonymous, anonymized, or remailed mail?

Is any encryption used? (PGP)

Are any digital certificates used?

Are any digital signatures used?

Mail Client

Does the client have automated virus checking?

What client email application/s are used to read the mail?

Are there any policies pertaining to the configuration of the client side software? If so, what are they?

What is configured by the SA and what is left up to the user?

Are any scripts used?

Are any personal certificates used? Can they be transferred?

Are passwords used?

Conclusion

The complexity of modern enterprises, their reliance on technology, and the heightened interconnectivity among organizations are rapidly evolving developments that create widespread opportunities for theft, fraud, and other forms of exploitation by offenders both outside and inside an organization. Internal and external perpetrators can exploit traditional vulnerabilities in seconds.

As detailed in this paper, it is envisioned that using the vulnerability assessment aids on a regular basis, along with immediate response to problems identified will alleviate these risks. Routine vulnerability assessment, therefore, should be a standard element of every organization's security policy.

Richard H. Wiens holds the position of Senior Secure Systems Engineer with Getronics Government Solutions, LLC, based in the Netherlands. He has broad responsibility for defining, analyzing, and improving security requirements for system security needs, identifying security vulnerabilities, and conducting security certifications and accreditations. He has also been involved with the security-related issues inherent to Electronic Commerce since 1994.

Relevant Links

[Subscribe to the Incidents Mailing List](#)

SecurityFocus.com

[Subscribe to the FOCUS-IH Mailing List](#)

SecurityFocus.com

[Privacy Statement](#)

Copyright 2006, SecurityFocus