

IS AUDITING PROCEDURE

SECURITY ASSESSMENT–PENETRATION TESTING AND VULNERABILITY ANALYSIS

DOCUMENT P8

The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of the Information Systems Audit and Control Association® (ISACA®) is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance.

Standards define mandatory requirements for IS auditing and reporting. They inform:

- IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics for IS auditors
- Management and other interested parties of the profession's expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

Guidelines provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure. The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.

Procedures provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

CobIT® resources should be used as a source of best practice guidance. Each of the following is organised by IT management process, as defined in the *CobIT Framework*. CobIT is intended for use by business and IT management, as well as IS auditors; therefore, its usage enables the understanding of business objectives, communication of best practices and recommendations to be made around a commonly understood and well-respected standard reference. CobIT includes:

- *Control Objectives*—High-level and detailed generic statements of minimum good control
- *Control Practices*—Practical rationales and "how to implement" guidance for the control objectives
- *Audit Guidelines*—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met
- *Management Guidelines*—Guidance on how to assess and improve IT process performance, using maturity models, metrics and critical success factors

Glossary of terms can be found on the ISACA web site at www.isaca.org/glossary. The words audit and review are used interchangeably.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics for IS auditors. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his/her own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

The ISACA Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary. The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Any suggestions should be e-mailed (standards@isaca.org), faxed (+1.847. 253.1443) or mailed (address at the end of document) to ISACA International Headquarters, for the attention of the director of research, standards and academic relations.

This material was issued on 1 July 2004.

Information Systems Audit and Control Association 2003-2004 STANDARDS BOARD

Chair, Claudio Cilli, Ph.D., CISA, CIA, CISSP Value Partners, Italy
Svein Aldal Scandinavian Business Security AS, Norway
Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay
Christina Ledesma, CISA, CISM Citibank NA Sucursal, Uruguay
Andrew MacLeod, CISA, CIA, FCPA, PCP Brisbane City Council, Australia
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA NextLinx India Private Ltd., India
Peter Niblett, CISA, CA, CIA, FCPA WHK Day Neilson, Australia
John G. Ott, CISA, CPA Aetna Inc., USA

1. BACKGROUND

1.1 Linkage to Standards

- 1.1.1 Standard S6 Performance of Audit Work states, "IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met."
- 1.1.2 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate documented analysis and interpretation of this evidence."
- 1.1.3 Procedure P3 Intrusion Detection Systems (IDS) Review provides guidance.
- 1.1.4 Guideline G25 Review of Virtual Private Networks provides guidance.

1.2 Linkage to COBIT

- 1.2.1 COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility as well as to achieve its expectations, management should establish an adequate system of internal control."
- 1.2.2 COBIT *Management Guidelines* provides a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
 - Performance measurement—How well is the IT function supporting business requirements?
 - IT control profiling—What IT processes are important? What are the critical success factors for control?
 - Awareness—What are the risks of not achieving the objectives?
 - Benchmarking—What do others do? How can results be measured and compared?
- 1.2.3 COBIT *Management Guidelines* provides example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.
- 1.2.4 COBIT *Management Guidelines* can be used to support self-assessment workshops and can also be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
- 1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT information criteria.
- 1.2.6 The COBIT references located in the appendix of this document outline the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Procedure

- 1.3.1 Primarily intended for IS auditors—internal as well as external auditors—this document can be used by other IS security professionals with responsibilities in capacity of information security.
- 1.3.2 Modern businesses are organised as a set of core processes operating within supply and demand networks. Almost every organisation in the world is faced with increasing pressure for effectiveness and efficiency (i.e., higher quality requirements for products and services, increased revenue, cost reduction, new product development), a pressure for better, faster and cheaper processes. These increasingly complex operating networks are supported by available communication technologies (mainly the Internet), allowing businesses to focus on their core competencies and partner with others to deliver enhanced value to customers; thereby, complexity introduces multiple avenues of threats and vulnerabilities.
- 1.3.3 The transformation of the old processes is enabled by new communication channels. These channels provide new linking possibilities among different systems and networks, making them available to more people and letting the organisations and their processes interact (e.g., e-procurement and e-sourcing).
- 1.3.4 This document provides guidance for IS auditors who are required increasingly to audit or review perimeter and internal controls to provide reasonable assurance that all external and internal threats, including potential system compromises, are minimised by identification and correction of vulnerabilities detected in performing a penetration test and vulnerability assessment.
- 1.3.5 **This procedure is not a substitute for an internal audit including an organisationwide risk assessment and internal general controls and application audits of all critical infrastructures and applications, including those with financial statement implications. Weaknesses in a noncritical infrastructure and applications component could have a consequential impact on a critical infrastructure and application components; therefore, a system wide audit should be completed in its totality and not in a piece-meal fashion.**

2. PENETRATION TESTING

2.1 Introduction and Planning

- 2.1.1 The penetration testing scope determines whether the individual tasks should occur in phases or in single sequence. The IS auditor's review should begin with a formal threat assessment to ascertain the likelihood of any threats to the organisation resulting from, among other reasons, hardware and/or software failures, internal employee compromise or data theft, or outside attacks.
- 2.1.2 The risks associated with unauthorised access vary from financial loss; inappropriate release of personal, commercial or politically sensitive information; and reputation lost; to total loss of system control. The specific information system risk of unauthorised access to information resources includes loss of system availability, data and processing integrity, and information confidentiality.
- 2.1.3 The purpose of this procedure is to test controls that should be employed to protect against unauthorised access. Since methods used for unauthorised access vary greatly and are becoming more sophisticated, the procedures defined are general

in nature and should be supplemented, wherever possible, with techniques and tools specific to the environment(s) under examination.

- 2.1.4** The significant difference in the actions taken by an IS auditor performing penetration testing (beyond having management authority) and a hacker is that the former is searching for (via testing) as many potential vulnerabilities as the testing script/program mandates, while hackers ordinarily will search for a specific vulnerability(ies) to exploit to fulfil their goal of (typically) obtaining control, or disrupting the operation or availability of the system. The hacker is likely to continue to attempt to find additional vulnerabilities once one is found to obtain increased system privileges and to protect against the increased risk of detection. Therefore, while an IS auditor performing penetration testing has a greater overall scope for finding general vulnerabilities, the hacker is likely to attempt to exploit any identified vulnerabilities more extensively.

2.2 Record Keeping

2.2.1 Records should be in sufficient detail to support the findings and conclusions reached as a result of the testing to:

- Defend against accusations of unethical or unauthorised practices against the IS auditor performing the test
- Provide the organisation with a detailed description of the weaknesses and how they were identified and exploited
- Provide an audit log for future testing to provide reasonable assurance that vulnerabilities identified have been addressed
- Demonstrate the possibility and risk of unauthorised access from any determined/willing attacker possessing the skills

3. TYPES OF PENETRATION TESTING AND VULNERABILITY ASSESSMENT

3.1 Scope of Evaluation

3.1.1 There are several types of penetration tests that will, depending upon the circumstances, affect the scope of the evaluation, methodology adopted and assurance levels of the audit.

3.1.2 The individual (appropriate IT management) responsible for safeguarding the organisation should evaluate various alternatives, selecting that which provides the maximum level of assurance with the least disruption acceptable to the organisation (cost/risk analysis).

3.1.3 There should be agreement on the type of penetration testing to be carried out—intrusive or nonintrusive.

4. EXTERNAL PENETRATION TESTING AND VULNERABILITY ASSESSMENT

4.1 Internet

4.1.1 The purpose of Internet testing is to compromise the target network. The methodology needed to perform this test allows for a systematic checking for known vulnerabilities and pursuit of potential security risks. The methodology ordinarily employed includes the processes of:

- Information gathering (reconnaissance)
- Network enumeration
- Vulnerability analysis
- Exploitation
- Results analysis and reporting

4.1.2 There are several variations to the processes listed in section 4.1.1. However, a common, standardised and objective script is ordinarily followed and should provide a detailed and exact method of execution. In addition, the intricacies of new vulnerabilities and methods of exploitation require detailed study with a history of information to draw upon.

4.2 Dial-In

4.2.1 War dialling is the systematic calling of each number in the target range in search of listening modems. Once all listening modems are identified, brute force default password attempts or strategic guessing attempts are made on the username/password challenge (sometimes only passwords are necessary) to gain unauthorised access.

4.2.2 Access to the login screen banner is crucial to accessing any system. Some systems require only a password, which can be a vendor-provided default password or just hitting “enter.”

4.2.3 At times of poor configuration, even a login banner does not appear and access is granted directly devoid of any authentication mechanism.

5. INTERNAL PENETRATION TESTING AND VULNERABILITY ASSESSMENT

5.1 Goal

5.1.1 The goal of internal penetration testing is to ascertain vulnerabilities inside the network perimeter. The testing performed closely parallels that which an internal IS auditor will be assigned to audit, given the size, complexity and financial resources devoted to risk associated with lack of security concerns. The overall objective is to identify potential vulnerabilities within the internal network and weaknesses in controls in place to prevent and/or detect their exploitation by a hacker/malicious employee/contractor who may obtain unauthorised access to information resources or cause system disruption or a system outage.

5.1.2 The first phase relates to information gathering, which is comprised of public information search, googling, obtaining maximum information about business, employees, etc., thereby profiling the target. For instance this phase may result in obtaining resumes/CVs of employees which may be useful in understanding technologies employed at the attack site.

5.1.2 The first testing goal is to ascertain the internal network topology or footprint that provides a map of the critical access paths/points and devices including their Internet protocol (IP) address ranges. This is the network discovery stage.

5.1.3 Once critical points/devices are identified within the network, the next step is to attack those devices given the various types of known vulnerabilities within the system and operating software running on the devices (e.g., UNIX, NT, Apache, Netscape and

IIS). This comprises the vulnerability analysis phase.

5.1.4 Exploitation and notification is the third and final phase.

6. PHYSICAL ACCESS CONTROLS TO DATA CENTRE AND OTHER WORK SITES

6.1 Rogue Access Jacks

6.1.1 Identification of telecommunication access paths into and out of the organisation's premises, including communications rooms, and the data centre areas are critical to identifying potential methods to intercept, prevent or modify data communications. These access paths should be physically secured from unauthorised access and rendered inaccessible without the knowledge and specific permission of the organisation as well as specialised equipment.

7. SOCIAL ENGINEERING TESTING

7.1 Tests of Controls

7.1.1 Social engineering techniques are employed in an attempt to obtain information regarding perimeter network devices and their defenses (i.e., IP address ranges, firewalls and default gateways) as well as potential internal targets. The information gathered during the reconnaissance phase outlines the basis of this test. The purpose of this testing is to assess the ease of extraction of critical information from internal organisation resources and employees/contractors, or others with detailed knowledge of the organisation, without their becoming aware of the significance of the information obtained. Of particular interest is testing whether the organisation's help desk will assist an unauthorised or unidentified user.

7.2 Telephone Access

7.2.1 First, and most importantly, the more information that the individual performing the test has about the organisation, employee and network, the greater the likelihood of success of extracting information. The individual performing the test should have a script. For example, the individual performing the test may pose as one of the technical support personnel, whose name was obtained in an earlier help desk call seeking information pertaining to connectivity and, therefore, requesting network information. Typically, these social engineering efforts succeed when information obtained from one source is used in combination with information from a second, progressive source.

7.2.2 Using information obtained from the help desk in the example in 7.2.1, the test continues by having an auditor pose as an organisation employee over the telephone asking for a password reset/change. These tests are best performed using a telephone inside the organisation, as help desk/security personnel employees may be more willing to accept the masquerade and provide the information requested without detailed authentication/personal confirmation. Acting as an impatient, disgruntled or aggravated customer over the phone as well as other personal behaviours (i.e., telling the help desk employee that they need access to get information to their superior without specifying their name) may add to the likelihood of success.

7.2.3 Background information, such as the mother's maiden name, zip code or social security number, of the employee being impersonated by the individual performing the test is helpful. In addition, obtaining resumes/CVs of employees through an Internet search or a stranger headhunter approach could be of more help.

7.2.4 Impersonating a consultant/auditor and reaching IT staff directly without any introduction is another approach. Management should be aware and agree to this approach to prevent unnecessary troubles.

7.2.5 Nevertheless, it is recommended that if caught because confidential proprietary information is unknown, the tester should excuse themselves using some plausible justification (e.g., not feeling well, their boss needs them right away, do not have time right now). Each piece of information obtained adds to increase the likelihood of a successful penetration to a critical information asset.

7.2.6 Each organisation differs in its structure (i.e., centralised in the same geographical area vs. segmented over a large physical area under different management), size (i.e., medium size bank with 500-800 employees to large financial management organisation with over 10,000 employees), network complexity and security awareness (i.e., well-known organisation or federal agency that is continuously probed by port scanning). All types of testing are valuable in obtaining valuable and sensitive information by social engineering.

7.3 Garbage Viewing

7.3.1 Review of garbage disposal areas and bins for information can be a valuable source of sensitive security and overall organisational information that could be useful in a social engineering examination. Access to recycled paper bins should also be considered a source of critical information.

7.3.2 Physical harm is possible in going through an organisation's garbage, as there could be everything from sharp objects to hypodermic needles to hazardous chemicals. The penetration testing contract, if performed by external consultants, should explicitly allow for this type of testing.

7.4 Desktop Review

7.4.1 As noted previously, none of the information obtained using social engineering may be particularly relevant except when taken together with other information obtained via other tests defined in this procedure. The most important aspect when attempting to exploit individuals' naivete or lack of training for the security of organisation proprietary information is that there will always be someone who will divulge information and it is ordinarily only a matter of time before such an individual is contacted.

8. WIRELESS TECHNOLOGY BACKGROUND

8.1 Background and Risks Associated With Wireless Technologies

8.1.1 With the advent of wireless technology for transmitting data and voice, the well-known and relied upon controls instituted using perimeter devices are disappearing. Gone are the physical security controls, such as security guards, cameras and

locks, that were effective in protecting wired networks and data transmissions. The major vulnerabilities result from the users of wireless technologies not addressing the following:

- Reliance on WEP for encryption
- Wireless networks not being segregated from other networks
- Descriptive SSID or AP names being used
- Hard-coded MAC addresses
- Weak or nonexistent key management
- Beacon packets that have not been disabled or are “enabled”
- Distributed APs
- Default passwords/IP addresses
- WEP weak key avoidance
- DHCP being used on WLANs
- Unprotected rogue access points

The risks and threats associated with attacks against wireless networks are widespread including:

- Attacks where message traffic is captured and analysed and encryption keys cracked, i.e., initialisation vector—IV
- Resource theft, where Internet access is obtained that in return is used as a launch pad for other attacks, i.e., cyclindrical redundancy check (CRC-32)
- Denial-of-service due to signal interference and propagation of threat from viruses and worms

8.1.3 In addition, as with other types of technologies, the greatest weakness with wireless security is not the technical shortcomings but out-of-the-box insecure installations. The human factor is typically the weakest link.

9. WEB APPLICATION

9.1 Manual and Automated

9.1.1 Web application testing includes manual and automated testing of the portal site as an outsider with no login information. This testing compliments the external penetration testing. The goal of this testing is to gain an understanding of how individuals interact with the system in accessing sensitive data.

9.1.2 Additional testing may include testing of the portal site by an insider through a standard login account. The goal of this testing is to determine the ease of access to sensitive information that is not authorised by the login account (i.e., privilege escalation).

9.1.2 Identification and exploitation of vulnerabilities can be accomplished through the use of various commercial and open source vulnerability assessment tools.

10. SUGGESTED PROCEDURES

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Planning	Define the scope based on the nature, timing and extent of the evaluation.	
	Verify that no test will violate any specific law of local or national statute. Also, the auditor should consider obtaining a signed “authorisation form” from the organisation agreeing to the deployment of penetration testing tools and methods.	
	Investigate and use available automated tools to perform penetration testing and vulnerability assessments. These tools improve the efficiency and effectiveness of penetration testing.	
	Define the scope of the review by asking the following questions: <ul style="list-style-type: none"> ■ Will the chief information officer, computer security and IT personnel be told of the penetration test? ■ Will the audit testing focus on detecting control weaknesses from those accessing the information infrastructure from the Internet and dial-in access (external) or from inside the organisation (internal)? ■ How far into the network and information asset will the penetration testing be performed? For example, will the testing be performed to the extent of actually accessing the information assets or will it occur to an access check point (where access to the information assets is not accomplished but there is sufficient information that it could occur based on testing)? Will the test be intrusive or nonintrusive? ■ What level of overall system degradation, and for what duration, will be acceptable in performing the tests? ■ Can the test be performed off hours to avoid potential conflicts with causing critical system outage (e.g., executing nmaps against firewall off hours, such as Sunday morning, while web application services are not used)? 	
	Obtain access to a (public) vulnerability database, such as bugtraQ, packetstorm, etc. The tester should determine that any tools used are up to date with the latest vulnerability database.	
Skills Required	Possess sufficient technical knowledge of, and ability to recognise and/or detect different types and variations of, security flaws/bugs/weaknesses/vulnerabilities. For example, the individual should have an understanding of the controls required over dial-in penetration, denial-of-service, password cracking, buffer overflows and wireless, as well as have access to up-to-date vulnerabilities database services.	
	Possess strong knowledge of how various technologies work, such as firewalls and routers, intrusion detection systems, and various types of authentication mechanisms.	
	Possess working knowledge of application programming, such as JAVA, Visual Basic and C++.	
	Possess knowledge of various operating systems, such as UNIX, Linux, NT/2000, Windows and OS/390 (or its current mainframe version).	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Skills Required continued	Possess working knowledge of TCP/IP and networking protocols.	
	Possess working knowledge of web server software, including Microsoft IIS and Apache.	
	Possess knowledge in utilising the penetration tools selected to detect bugs and vulnerabilities.	
	Possess knowledge of the effect on the internal system of executing penetration and vulnerability tools, including the NMAP, ISS, Whisker, Nikto, WebInspect, AppScan, ESM and Root, Nessus.	
Agreements	Keep all records, including specific and detailed logging of all keystrokes and verbal discussions, of all activities during the penetration and vulnerability testing. These records should be in sufficient detail to recreate the test, if necessary.	
	Keep all records of the penetration testing, including the results, confidential as they are the property of the organisation. All records of the penetration and vulnerability testing should be maintained within the organisation's control. The individual performing the test should sign nondisclosure and code of ethical conduct statements with the organisation regarding the confidentiality of the scope of the test and results.	
	If the test is to be performed by external consultants, include a contract to protect the organisation. The contract should state the boundaries and scope of the work to be performed, the ownership of the results and test procedures, as well as require confidentiality and ethical conduct of the consultants. In addition, the external consultant should provide insurance and a "hold harmless" clause to mitigate risks as a result of an inadvertent release of information.	
Scope Questions	Does the testing consist of evaluating the control environment based on penetrating the information infrastructure from inside vs. outside the network perimeter? For example, if the test consists of evaluating the firewall rule set based on attempted access to penetrate the network from the Internet, the evaluation is focused on determining the access control from outside the network perimeter. Testing of perimeter controls is limited in scope to the physical and logical controls that safeguard the information assets from those threats external to the organisation. However, once the perimeter security controls are compromised, a decision should be made, whether to continue testing to determine the adequacy of the controls over the target information systems. Conversely, the vulnerability testing may be focused on evaluating the internal control environment to prohibit access to information assets from inside the organisation.	
	Is the appropriate level of management, including IT security, notified of the penetration or vulnerability testing? If a formal announcement is made of the testing, strong cooperation and more thorough evaluation may be achieved. Conversely, unannounced testing may better represent the actual risks and management's response based on real-world threats from unauthorised access attempts. It is essential to assess the best-case scenario and level of assurance needed.	
	Are the individuals performing the test provided information about the organisation in advance? This question goes with whether management is notified of the nature and scope of the test. However, there are times when just the executive or high-ranking IT management is notified of the test and it is not announced to the staff. Nevertheless, if information is provided (i.e., network topology) and used by the tester, a more exact review of the target systems and processes can be examined, possibly resulting in better identification of risks and vulnerabilities. However, providing insider information may result in difficulty in understanding the depth of the vulnerabilities and their likelihood of exploitation. In addition, the IP ranges, if provided by management, should also be tested.	
Internet Penetration Testing	<p>Network enumeration is the information obtained: network resources and shares, user logins including generic installation (out of the box) hardware and software vendor user IDs, IDs and their groups, and applications and banners. The steps to consider are:</p> <ul style="list-style-type: none"> ■ Identify the domain name, IP address range and other critical information. Ordinarily, the "who is" query is used, which typically provides the address of the target network (i.e., domain name servers and IP address mapping), administrative contact and billing contact. The individual executing the "who is" query should provide reasonable assurance that all listings are obtained, and not just the first 50 items, which may require grouping the names into plurals or modified organisation names. ■ Identify IP address ranges that may be owned by the organisation. This is typically done by querying Internet number registries such as ARIN, RIP, APNIC and LACNIC. ■ Identify external e-mail servers by gathering MX record information from DNS servers. ■ Attempt a zone transfer between all systems identified as a DNS server (including back-up servers) to obtain the network IP listing and the machine host names. A zone transfer requests the complete list of matched IP addresses and host names stored within a DNS for a specified domain. In addition, the "nslookup," which is supported by both the UNIX and Windows platforms, may also be used to perform a zone transfer using a DNS server that is authoritative for the domain of interest. In addition, the machine's host names may indicate its purpose (i.e., mail server and firewall), which is one more critical piece of information. Recent technologies prevent the ability to perform a zone transfer without the initiating device. ■ Determine whether the organisation has outsourced its domain name function to an Internet service provider (ISP). In cases where this function is outsourced, it is recommended that the terms of the penetration test clearly state whether the hosted system is within the scope of the engagement. ■ Notify network staff that a penetration test may be underway because zone transfer can be detected. ■ Use ICMP (ping) or TCP ping (with a full or half TCP handshake) sweeps to determine which machines for IP addresses are "up" or "live." Though this step may provide critical information 	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Internet Penetration Testing continued	<p>regarding which devices are active, there is a likelihood that perimeter security devices or firewalls may drop the ICMP traffic to the host. It may be filtered and dropped with a response indicating the device is down, when it is not. It is recommended that randomising the order of the IP addresses being pinged helps avoid detection, as does varying the NMAP. NMAP is a popular tool used for UNIX-based systems and Pinger, and Ws PingPro Pack are used in Windows-based environments for performing Ping sweeps.</p> <ul style="list-style-type: none"> ■ Use the traceroute method to identify the paths from the Ping packets to the destination target. The routes can then be traced to the destination live hosts, detected using the Ping sweeps to derive an estimated map of the organisation's architecture topology. The two commonly used tools are traceroute and tracert, available for both UNIX- and Windows-based operating systems. The purpose of this method is to identify the common and uncommon "hops" prior to reaching the destination targets, which could represent such things as firewalls, filtering routers or other gateways, load-balancing devices, or web redirectors. It is not uncommon for network segments to have multiple connections to the Internet—unknown to the network group. However, these uncommon paths can lead to network compromises, if uncontrolled. ■ Send "bogus" e-mail messages to domains owned by the organisation in an attempt to receive a returned e-mail. Review the header of returned e-mails to determine possible network paths. 	
	<p>To perform a vulnerability analysis:</p> <ul style="list-style-type: none"> ■ Assess possible methods of attacks based on identification of vulnerabilities. To do this, identified machines within the target network are examined to identify all open ports, the operating systems (OS), the applications and their hosts (including version number, patch level and/or service pack). In addition, this information is compared with Internet vulnerability databases to ascertain what current vulnerabilities and exploits may be applicable to the target network. ■ Identify the type of OS employed by target hosts. For those target hosts identified in the network enumeration phase, the NMAP tool can be used to identify the type of OS employed. The type of OS employed is critical in predicting the types of service available and then to tailor the targeted analysis of service rendered through that port, which, when executed, will determine if specific vulnerabilities exist. In conjunction with this step is the need to obtain a current list of vulnerabilities for the OS employed by searching the OS vendor's web site and vulnerability databases to obtain details of these vulnerabilities. ■ Obtain permission to execute a port scan for those destination target hosts that are "live." A port scan may be needed on all possible ports (1-65535), if the security group is aware of the penetration testing. The list of ports should include applications that have known vulnerabilities. Ports examined should relate to weaknesses, vulnerabilities or information gathering. For example, the ports for file transfer protocol (FTP), Telnet, and RealSecure (ports 21, 23 and 2998) are often selected to attempt to exploit vulnerabilities. NMAP is the standard tool and can be programmed to execute a port scan for those destination target hosts that are "live" (from a port scan). Port scanning is clearly unethical without the express permission of the port owner. Port scanning, as with many other vulnerability tests, is a technique that may be employed by hackers, and should alarm the security group of a potential attempted penetration. ■ Perform an application enumeration to identify assigned services (applications) of ports. In addition to the port scan, the specific identification of assigned services (applications) to a port is known as application enumeration. Knowing which applications the target hosts are running goes a long way toward performing a vulnerability analysis. Ordinarily, the applications are run through the Internet. Find a list of known vulnerabilities and exploits for these applications, which often comes from the vendors themselves and vulnerability databases. Application enumeration also involves banner grabbing, which may be helpful in identifying running applications. This can be done with many applications, including Netcat, which runs from either the UNIX or Windows command line; Telnet; and What's Running, a Windows GUI tool. Examples of common sources of information about system and application software vulnerabilities and exploits are Bugtraq lists, Packetstorm and SecurityFocus. ■ Run commercial or open source network vulnerability assessment tools to verify results. Popular tools include Nessus, ISS Internet Scanner, Foundstone's FoundScan, eEye's Retina Scanner and GFI's LANguard. 	
	<p>Exploit vulnerabilities identified in the vulnerability analysis to attempt to gain root or administrator-level access to the target systems or other trusted user account access as follows:</p> <ul style="list-style-type: none"> ■ Document all relevant information upon access to the command line of a targeted system, via the access points identified in the vulnerability analysis, including the host and directory or share name to which access was gained; the host from which access was gained; date, time and the level of access; and finally the security hole(s) that were exploited to gain access. ■ Launch attacks against other systems on the network from the host that was compromised. If possible, a tool kit is installed on the exploited hosts that are tailored to the operating system of the other targeted machines to ascertain their vulnerabilities. The tool kit may include Netcat, password crackers, remote control software, sniffers and discovery tools, which can be executed from the command line. At this point, the method of Internet (external) penetration merges with internal testing methods described in section 5. ■ Notify the organisation if the access level is achieved, allowing installation of critical viruses that could result in consequential system outage. 	
Dial-in	Gain penetration by dialing in over the telephone line that is listening for incoming connections, and log into the host machine. Example of vulnerabilities searched for may include:	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Penetration Testing	<ul style="list-style-type: none"> ■ Modems attached to machines, such as routers, that are used by the hardware and software vendors to maintain it (i.e., installation of patches) ■ Rogue modems that are connected to actively listening users' desktops ■ Modems where remote management tools are installed, such as PCAnywhere ■ Modems that are authorised but insecurely configured 	
Dial-in Penetration Testing continued	<p>Gather the groupings of phone numbers used to make calls. Sources include phone books, online directories, company brochures and literature. Internal telephone directories may be particularly valuable, if accessible. These may be based on block(s) of phone numbers within a specified range that may be geographically assigned:</p> <ul style="list-style-type: none"> ■ Find where the target organisation physically resides, which will define its area code and, to a lesser extent, its prefix. ■ Attempt to obtain these numbers independently of the organisation to ascertain the difficulty. It may require a level of social engineering. 	
	Identify listening modems by calling each number in the target range randomly. War dialing software can be employed to dial and record the responses to determine if there is a modem listening.	
	After detecting a modem that is listening, gain unauthorised access by making brute force default passwords or strategic guessing attempts on the username/password challenge. War dialing software can be set to attempt to gain login access by using the largest list possible and/or selective list of default user IDs and passwords. The selective default list may also include strategic guesses of the user ID/password pair. For example, for a Cisco router, the username/password pair may be Cisco/Cisco or enable/Cisco or, when only a password is asked c, cc, cisco, and Cisco router, may be attempted. Vendor provided default user ID/password pairs should be attempted, as these are very often not changed or disabled.	
	Determine whether sniffers and keyboard loggers are installed on web devices within the demilitarised zone (DMZ) to pick up user IDs and passwords.	
	Consider whether PCAnywhere is being used, configured to allow connection without authentication as long as the calling client is using the PCAnywhere.	
Internal Penetration Testing	<p>Perform a network discovery test using the following steps:</p> <ul style="list-style-type: none"> ■ Perform a Ping sweep to identify live hosts. Popular tools include NMAP Pinger, NetScan tools and WS_Ping ProPack tools. ■ Also, if possible, install sniffers on the hosts that have been compromised in the external penetration test that identifies ARP tables, SNMP data and routing information. ■ Attempt to perform a zone transfer to learn internal IP addresses and computer names, which may indicate the purpose of the host. ■ Attempt to perform a tracer route to fine tune the target list of hosts deemed critical. ■ Guess the community strings or whether it was set to public or private to obtain SNMP information, which includes routing tables, protocols, error logs, and other system and network data, to build an attack. Also attempt to guess commonly used community strings (e.g., Cisco, {company name}, router, switch, network) ■ After completing the above, obtain authorisation from the security group to install host-based automated discovery tools that provide a full listing of vulnerabilities. Popular tools include Enterprise Security Manager (ESM), ISS, etc. 	
	<p>Perform a vulnerability analysis using the following steps:</p> <ul style="list-style-type: none"> ■ Execute a port scan and banner grabbing programs on the target hosts to identify active services. This is comparable to external penetration testing. This step can be performed in conjunction with the Ping sweeps using NMAP. ■ Test the individual known vulnerabilities for each type of system software, in conjunction with the open ports for exploitation. For example, known anonymous FTP vulnerabilities should be tested to determine if these weaknesses could be exploited by utilising an exploit script and subsequently installing a root kit containing Netcat to open up a command prompt on a particular point. There are numerous known vulnerabilities that constantly expand. ■ Obtain authorisation from the security group to install automated discovery tools that provide a full listing of vulnerabilities. These tools include CyperCop, Enterprise Security Manager (ESM) and Internet Security Scanner (ISS) and Nessus. ■ Generate a schedule of IP addresses host names, types of system software (i.e., UNIX and NT), open ports and application (Netscape and IIS and Apache). 	
	<p>Perform the exploitation and notification using the following steps:</p> <ul style="list-style-type: none"> ■ Determine the level of attack that the organisation would desire and approve. ■ Determine the level of attack based on the level of access obtained on the open ports and the target hosts identified by the discovery and analysis stages, or on the basis of information provided by the organisation. For example, if the target host is UNIX-based, the next step after gaining access to this device could be to attempt to crack the password file. In addition, if the attacker can obtain access to other devices and valuable organisation data without detection, the penetration was a full success. ■ Notify the organisation if access level is achieved, allowing installation of critical viruses or root kits or other tools or software that could result in consequential system outage or to demonstrate the ability of an attacker to retain unauthorised access devoid of detection. ■ Record all vulnerabilities noted and provide to the organisation for immediate follow-up at the conclusion of the penetration test/vulnerability analysis. 	
Physical	Search for rogue access jacks that can be exploited. Identify telecommunication access paths into	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Access Controls Physical Access Controls continued	and out of the business and data centre area. Access paths should be buried or cancelled and not accessible by the general public. Attempt to identify cabling in ceilings or closets where an unauthorised tap can occur, though this may not be always possible especially given the use of fiber optic cable.	
	Perform brute and selective access to default user IDs once access to the network is physically obtained.	
	Obtain physical access and initiate social engineering as defined in section 7 of this procedure: <ul style="list-style-type: none"> ■ Without authentication as an employee one should attempt to obtain unimpeded access. For those organisation sites with physical security via mechanical, electronic or physical guard, this testing can be accomplished in multiple ways including piggybacking into the site with a legitimate employee or signing in without an escort and walking directly into the data centre or business work sites. ■ Standard business practice should restrict direct unimpeded access to all work areas. ■ The consulting agreement or internal auditor performing the test should explicitly require this evaluation. ■ A data centre audit should be performed to evaluate all the physical controls to the data centre and other work sites. 	
	Create burs around the data centre complex to avoid intruders or interlopers from obtaining transmission signals.	
Social Engineering Testing	Test controls to prevent social engineering or circumvention of logical security measure in place by masquerading as an individual calling over an internal phone with a business need requesting critically sensitive information or access to basic computing services.	
	Explicitly allow the penetration testing contract, if performed by external consultants, to test garbage disposal areas.	
	Review confidentially policies and practices to ascertain whose responsibility it is for the disposing and shredding of organisation-related information in hard copy form. Safeguards for the disposal of data are critical.	
	Review measures for the disposal of magnetic media holding sensitive data.	
	Review individual employee work areas as well as printer baskets for propriety information, such as user ID, other employee's information and computer names, if physical access to the work area is obtained. Sticky notes and to-do lists can be sources of important information.	
	Obtain a building and floor schematic of critical areas. Work areas, such as the treasury and disbursement departments as well as executive offices, are primary targets.	
	Determine whether individual desktop computers have a screen saver and work desks are locked. Provide reasonable assurance the scope of the work does not break any laws.	
Wireless	Find and map the wireless networks into a street or physical geographic area map. The tools needed to perform a penetration test of a wireless network may include a laptop/PDA, a wireless NIC (ORiNOCO or Lucent PC, Card Dell TrueMobile 1150, Avaya Wireless PC Card, Compaq WL110, Enterasys Roamabout Elsa Airlancer MC-11), freeware software, and an antenna and GPS. One technique used for finding a wireless network is War Driving. This is done by detecting the beacon and broadcast. War Driving is used to capture and map wireless band signal.	
	Crack the WEP (Wired Equivalent Privacy) keys by using automated tools such as WEPCrack and AirSnort. The techniques used include IV Collisions and Weak key packet capture.	
	Sniff and analyse the network traffic to ascertain the number of packet passes, SSID, etc. There are a variety of automated tools, such as PrismDump, Iris, AiroPeek and Sniffer Wireless.	
	After the key is known, reassemble the packet to complete the penetration test. Document all issues noted for management review. Before this test, it is best to consult legal representatives practicing within the individual countries and, where necessary, local and state municipalities to provide reasonable assurance that performing this test will not violate any laws or regulations due to picking up information packets from other unintended targets.	
Web Application	Analyse the web application and environment by first crawling through the web pages to gather the information including mapping of all pages and general understanding of all functionality to ascertain risk. Specifically, manually surf the application with a recording proxy (e.g., webproxy, ebsleuth) to find hidden data and locate form weaknesses. In conjunction with this survey, complete the following: <ul style="list-style-type: none"> ■ Review inventory SSL/TLS ciphers to determine accordance with policies or standard industry practices. ■ Analyse session tracking including mechanism and session ID. ■ Identify authentication methods employed, including client certificates, auditing and revoking certificates, use of encryption or HTTP basic authentication and deployment of SSL. ■ Identify sign-on and sign-off (use of anticaching techniques and session inactivity cause automatic sign-off) mechanisms. ■ Identify all points of user input by recording every form element, specifically: <ul style="list-style-type: none"> – Test SQL injection – Attempt buffer overflow to gain control – Cross-site scripting (XSS) – Special characters (pipes, returns, etc.) – For numeric input try 0, a negative value, a really large value ■ Record any verbose error messages. In addition, test any HTTP headers being used as input 	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Web Application continued	<p>such as:</p> <ul style="list-style-type: none"> - Cookie, Referrer, Host, User-agent - Record permutation list used - Record any verbose error messages - Test user input embedded into URL for POST <ul style="list-style-type: none"> ■ Review for hidden content or information leakage in Web Application Output <ul style="list-style-type: none"> - Search for client-side code for unnecessary information (meta tags, comments). - Ascertain if HTTP from server for unneeded information (Server:, X-). - Determine if Java applets and similar are decompiled. - Retrieve robots.txt file for each known directory and review. ■ Review security over session IDs including the following tests: <ul style="list-style-type: none"> - Determine if they are random, not related to user information, large enough to avoid brute force, perishable, transmitted over secured path, controls to prevent tempering, and have a detection mechanism. - Determine that cookies with session IDs are marked "secure" (encrypted), nonpersistent (not stored on hard-drive), reasonably limited to path and domain and, if appropriate, digitally signed. - Verify URLs with session ID are sent with encryption, such as SSL. ■ Review controls over sign-on including the: <ul style="list-style-type: none"> - Warning banner and error messages to warn against an unauthorised hacking attempt - Generic message does not providing specific knowledge of which is incorrect when a login is made with an invalid password or login account - Encryption of initial login involving credentials - Timeout after a period of inactivity to prevent half open sessions - Lockout mechanism for invalid login attempts to minimise exposure to brute-force attacks - Lock mechanism does not result in denial of service of a substantial number of suspended login accounts, rather it provides notification of attack resulting in an escalation process ■ Determine if all information transmitted is encrypted, such as verifying lock is shown on web browser. Ascertain if all pages sent and received are encrypted. <p>Collectively review results of the survey evaluation and results of the portal testing steps to ascertain the vulnerabilities that could be exploited to gain access to sensitive information by an outsider with no information of the system and no login account andan insider with knowledge of the system with a login account.</p> <p>Note: Since there are significant numbers of exploits detected via port 80, as time goes by, it is recommended that those performing this test possess current knowledge that would exceed that which is defined in various research documents, white pages and web sites. In addition, there is a series of audit testing of the web servers, including standard access control list evaluation and TCP/IP weakness, that should be performed and are included in other sections of this procedure.</p>	
	<p>Run commercial or open source application vulnerability assessment tools to verify results. Popular tools include Nikto, WebInspect, ScanDo and Appscan.</p> <p>There are numerous potential vulnerabilities that could be detected by performing the above testing. Accordingly, the second step is to exploit potential vulnerabilities, which would include, but are not limited to, the following:</p> <ul style="list-style-type: none"> ■ Alter contents of cookies (e.g., altering the parameters passed to the application through a URL) resulting in access to sensitive information or impersonating another user. ■ Change JavaScript within the application or hidden form files on application forms, parameter tampering, SQL injection (passing SQL code into an application that was not intended), cross-site scripting (entering executable commands into web site buffers). ■ Insert code into text fields to take control of an application. ■ Directly access a web page that can ordinarily only be reached through authentication by a brute force attack. Collect user IDs where wrong passwords are entered and execute the dictionary against them. ■ Directly exploit backdoors and debug options including executing debug syntax on URLs (e.g., there is a listing of vulnerabilities on various web sites including CERT and vendor sites, such as www.nstalker.com). ■ Exploit any configuration errors in third-party applications, such as web or database servers. Specific attempts should be made to exploit web server default configuration vulnerabilities that are known. ■ Insert scripting languages in a text field that other users will see. ■ Pass excessive data in an application request (e.g., sending large numbers of characters to a web site form/field). 	
Report	<p>Prepare report in accordance with ISACA IS Auditing Standards including:</p> <ul style="list-style-type: none"> ■ Defining the scope ■ Objectives ■ Period of work performed 	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Report continued	<ul style="list-style-type: none"> ■ Nature, timing and extent of the penetration testing and vulnerability analysis performed ■ Conclusion as to the effectiveness of controls and the significance of vulnerabilities identified 	
	Follow-up to provide reasonable assurance that controls were implemented and security holes were plugged on all known vulnerabilities.	
	Perform a specific process and attribute review of perimeter firewalls and routers, and discuss risks identified with management.	

11. EFFECTIVE DATE

11.1 This guideline is effective for all information systems audits effective 1 September 2004. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.

APPENDIX

CobIT Reference

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT information criteria:

- PO6—Communicate Management Aims and Direction
- PO9—Assess Risks
- A13—Acquire and Maintain Technology Infrastructure
- DS5—Ensure Systems Security
- DS7—Educate and Train Users
- DS10—Manage Problems and Incidents

The information criteria most relevant to a penetration testing and vulnerability assessment are:

- Primary: confidentiality, integrity and availability
- Secondary: efficiency and reliability

References

Bosworth, Seymour; Michel E. Kabay, Editor; *Computer Security Handbook*, 4th edition, John Wiley & Sons, Indianapolis, Indiana, USA, April 2002

The CERT Guide to System and Network Security Practices, 1st Edition, Addison-Wesley Publishing Co., June 2001

e-Commerce Security: Security the Network Perimeter, IT Governance Institute, Rolling Meadows, Illinois, USA, 2002

Klevinsky, T.J.; Scott Laliberte; Ajay Gupta; *Hack I.T.—Security Through Penetration Testing*, Addison-Wesley, Boston, Massachusetts, USA, June 2002

Kreutz, Vines; "The CISSP Prep Guide;" John Wiley & Sons, Inc.; 2001

Rhoades, David; "Hacking and Securing Web-based Applications," Maven Security Consulting Inc., 12th USENIX Security Symposium, Washington DC, USA, 4-8 August 2003

Scambray, Joel; Stuart McClure; George Kurtz; *Hacking Exposed—Network Security Secrets & Solutions*, 2nd Edition, Osborne/McGraw-Hill, Berkeley, California, USA, 2001

Yeager, Nancy J.; Robert E. McGrath; *Web Server Technology*, Morgan Kaufmann Publishers Inc.

Copyright © 2004
 Information Systems Audit and Control Association
 3701 Algonquin Road, Suite 1010
 Rolling Meadows, IL 60008 USA
 Telephone: +1.847.253.1545
 Fax: +1.847.253.1443
 E-mail: standards@isaca.org
 Web site: www.isaca.org