Whole of Victorian Government Guideline
Information Security

Penetration testing

Guideline

Guideline for department and agency implementation of the Information Security Penetration Testing standard SEC/STD/03.

Keywords:	Information security penetration testing; SEC/STD/03; guideline; SEC/GUIDE/03	
Identifier: SEC/GUIDE/03	**Version no.:** 1.0	**Status:** Final
Issue date: N/A	**Date of effect:** 1 May 2010	**Next review date:** In progress
Owner: Government Services Division Department of Treasury and Finance Victorian Government	**Issuing authority:** Government Services Division Department of Treasury and Finance Victorian Government	

Overview

In November 2009 the Department of Treasury and Finance (DTF) published the whole of Victorian Government (WoVG) information security standard on penetration testing, SEC/STD/03[1]. This standard describes the requirement for annual penetration testing of all externally facing applications and infrastructure, as well as business-assessed sensitive internal systems. It requires all inner budget departments and agencies to prepare a response to DTF:

- by May 2010 (now 30 June 2010) outlining the initial work plan for penetration testing; and
- annually on the results of penetration testing (1 November).

Subsequent departmental penetration testing programs of work should be included in the overall departmental program of work in the response to the Information Security Management Framework SEC/STD/01[2].

Audience

Information security is the responsibility of all staff. These guidelines are therefore produced for the benefit of information owners, and the IT staff involved in compliance with SEC/STD/03.

Context

This guideline will assist departments in their consideration of compliance with SEC/STD/03 and should be read in conjunction with that standard.

Suggested approach

Phase 1: plan and consult

The success of the penetration test will depend on a comprehensive planning and preparation phase.

1. **Define the objectives of the proposed penetration test**
   Document what the business is trying to achieve through the test. The objective will play a large part in defining the scope of the test.
2. **Consider the legal and contractual obligations**
   These obligations could potentially limit the time and nature of the test. Legal obligations, contractual service level agreements, availability requirements in contracts, throughput service level agreements and similar conditions will impact the scope of the test.
3. **Ensure findings are covered under strict non-disclosure agreements**
   Findings of penetration testing may contain sensitive security weakness information. Ensure that the project in general and the findings specifically are covered by the strictest non-disclosure agreements.
4. **Discuss the risks**
   Risks of conducting the penetration test need to be discussed with the stakeholders. This includes IT staff, application owners, business stakeholders and executive management. The outcomes of the risk discussion may have an impact on the scope of the test.

[1] Department of Treasury and Finance *SEC/STD/03 Information Security Penetration Testing*, November 2009, https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security

[2] Department of Treasury and Finance *SEC/STD/01 Information Security Management Framework*, April 2009, https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security

5. **Finalise the scope**
   Once the objective, legal and contractual obligations are completed and the risks discussed with stakeholders, finalise the actual scope of the penetration test. The scope should clearly define the timing, extent and nature of the test, including target systems, whether it needs to be a 'black box' or a 'white box' test etc. The scope should also specify the success criteria against which the department can measure results.
6. **Notify appropriate stakeholders involved**
   Appropriate stakeholders need to be identified. For example: internet services providers may need to be informed so that they don't automatically block sniffer packets; business executives may need to be informed if there is risk of system performance degradation; HR may need to be involved if a social engineering test is to be performed.
7. **Develop and approve the test plan**
   Develop a comprehensive test plan. Once this detailed, step-by-step plan is developed, business executives (the information owners) and other relevant stakeholders are required to approve it.

Phase 2: reconnaissance and information gathering

A penetration tester will generally use the same techniques and processes used by an external hacker. The first and most important step in penetration testing is gathering base information on the target system/network. This is called passive reconnaissance. This phase consists of:

1. gathering publicly available information;
2. gathering information from other sources; and
3. identifying target details.

Phase 3: device/network enumeration and vulnerability scanning

The authorised attack is carried out using public, customer and professional tools to identify the vulnerabilities that could be exploited by potential attackers.

1. Scan target network and identify devices;
2. Identify device operating systems;
3. Scan devices and networks for vulnerabilities;
4. Identify services/open ports;
5. Determine landscape of target network;
6. Identify vulnerabilities; and
7. Review logs.

Phase 4: analysis of recommendations

In this critical phase, the test team analyses the information and reports high-risk vulnerabilities and recommended controls to the sponsor. The final report must map the findings (the risks) to the department if the vulnerabilities had been exploited and threats were realised. The final report must contain the objectives and scope of the penetration test, findings and recommendations from each phase and the relative priority of these recommendations.

1. Assess weaknesses and impacts;
2. Identify controls/strategies for remediation;
3. Perform cost/benefit analysis;
4. Develop remediation action plan; and
5. Integrate action plan into the departmental risk management process.

Scoping considerations

A non-exhaustive list of criteria to consider for testing of known and unknown vulnerabilities is given in the table below. The actual testing will depend on the purpose and scope of the test. Additional vulnerabilities will arise from time to time, while some existing vulnerabilities will be made redundant due to dynamically changing technologies. Therefore, this list acts as a guide only. Departments and agencies remain responsible for determining the scope and extent of their penetration testing.

Physical access controls	Identify access points into the: • premises; • server room; and • network. Determine whether: • adequate access controls are provided on doors; • alarm monitoring controls are in place; • opportunities for 'tailgating' exist; • opportunities for 'shoulder surfing' exist; • adequate access controls to the server room exist; • server security containers (racks) provide adequate access controls; • any logging, auditing and monitoring is being conducted and how long the logs are maintained; • 'dumpster-diving' can reveal any information; • classification-based physical containers and secure areas exist[3]; and • written sensitive information such as passwords or configuration details etc. are lying around on desks or desktops. Determine who has access to control mechanisms to the premises, server rooms, racks etc.
Social engineering	Identify whether: • opportunities for 'tailgating' exist; • opportunities for 'shoulder surfing' exist; • confidential/privileged information is available through telephone enquiries; • confidential/privileged information is available from staff; and • policies exist for confidentiality. Identify staff awareness of security requirements. Check for sensitive conversations in public areas e.g. canteens, coffee shops, breakout areas.
Wireless devices	Look for rogue wireless devices on the network. Identify: • wireless endpoint devices on network/accessible in the area; and • the wireless Access Points accessible in the area. Determine: • the encryption mechanisms used; • the Authentication mechanisms used; • whether authorisation mechanisms (password length/complexity) are adequate; • the model and firmware versions of wireless devices to see if vulnerabilities exist; • whether wireless access points/devices are physically accessible; • the antenna type used on Access Points and their orientation; • whether parameters on wireless devices are configured correctly; and • the services/ports open on wireless devices.

[3] Refer to the Australian Commonwealth Government's Protective Security Manual (PSM) produced by the Commonwealth Government's Attorney General's Department: http://www.ag.gov.au/www/agd/agd.nsf/Page/RWPE30AA68A4D5313EACA2571EE000AAF9F and the Australian Commonwealth Government's Department of Defence Information Security Manual (ISM), September 2009, produced by the Defence Signals Directorate: http://www.dsd.gov.au/library/infosec/ism.html

Operating systems	Determine: • the version and service pack levels of identified devices; • what ports are open on servers and workstations; • what privileged accounts exist on servers and workstations; • what privileged groups exist on servers and workstations; and • what local and network user accounts exist. Determine whether: • antivirus controls are in place and up to date; • firewall controls are in use on local systems; • security auditing is being conducted on local systems and servers; • the authorisation mechanisms in place (password length/complexity) are adequate; • the authentication mechanisms in place are adequate; • rogue services are running on servers; and • unauthorised applications are running on servers / workstations. Check: • for user accounts not accessed in more than 30 days and the reasons; and • details of privileged users—how many, what access, need, etc.
Network infrastructure	Determine: • what devices are discoverable on the network; • what network infrastructure is physically accessible; • the model and firmware versions of network devices to see if vulnerabilities exist; • what ports are open on network devices; • what services are available; • what authorisation mechanisms (password length/complexity) are in place; • what authentication mechanisms are in place; and • what local user accounts are on devices. Determine whether: • rule-sets on applicable devices are configured appropriately; • devices are configured appropriately with minimum access requirements; • auditing is being conducted on network devices for access and changes; and • physical connection to the network is accessible.
Security devices	Test authentication and authorisation services. Determine: • what security devices are discoverable on the network; • what security devices are physically accessible; • what access is possible on security devices; and • the model and firmware versions of security devices to see if vulnerabilities exist. Determine whether: • security incidents and concerns are logged, monitored and reported; • any controls exist to deter or prevent unauthorised access; • antivirus controls are in place and whether the virus signatures are up to date; and • network filtering devices exist. Check for adequacy of rule sets, access control lists, etc.

Web applications	Determine whether: • web services are hosted internally or externally by third party; • identified websites are susceptible to known vulnerabilities; • confidential information is accessible via websites; and • appropriate secure communication channels exist between client and web server. Determine: • what applications are hosted on corporate servers; • the requirements for user access to websites, including; o the authorisation mechanisms in place; and o the authentication mechanisms in place; • patch levels on web applications.
Applications	Determine: • what applications are on the network and their purpose; • the version and release number of applications; • the requirements for user access to applications, including; o the authorisation mechanisms in place; and o the authentication mechanisms in place; • what information is accessible from the applications. Determine whether: • any known vulnerabilities exist within the identified applications; • the controls around the applications are appropriate for the classification level of the information stored within them; • databases are associated to applications; and • other applications share information with the application being assessed.
Incident detection and response	Determine whether: • incidents have been detected and what actions were taken; • a policy and procedure exist to respond to incidents; • staff are aware of policy and responsibilities in responding to incidents; and • incidents are logged and audited. Determine the timeframe for incident detection to incident response.
Information security policy	Determine whether: • an information security policy exists; • the information security policy is enforced; and • controls in place reflect information security policy. Determine: • adherence to information security policy; and • user awareness of the information security policy
Databases	Determine: • what databases exist on the network • the requirements for access to databases, including o the authorisation mechanisms in place o the authentication mechanisms in place • what privileged accounts exist on databases • the assignment of responsibilities of each privileged account Determine whether transaction logging and auditing is being performed.

Reporting template

SEC/TEMP/03 is to be used for the annual reporting of penetration test results. The template should be downloaded, completed, saved and returned to info.cio@dtf.vic.gov.au:

https://www.dtf.vic.gov.au/CA257310001D7FC4/WebObj/201005SECTEMP03Informationsecuritypenetrationtestingcompliancereportingtemplate May2010/$File/201005%20SEC%20TEMP%2003%20Information%20security%20penetration%20testing%20compliance%20reporting%20template%20May%202010.pdf

Glossary of terms and abbreviations

Term	Meaning
Internal penetration test	Penetration testing the systems and services that are accessible and exploitable from inside an agency level network, and identifying what information and systems can be viewed, and what vulnerabilities exist.
External penetration test	Penetration testing the information, systems and vulnerabilities that are accessible and exploitable from outside the physical bounds of the network. For example, determining what can be identified and accessed from a public network.
Vulnerability	A flaw or weakness that can be exploited to gain an advantage.

Version history

Version	Date	GSD TRIM ref	Details
1.0	13 May 2010	D10/37178	First promulgated