



IT Security Handbook

Risk Assessment: -
Procedures for Information System Security
Penetration Testing and Rules of Engagement

Risk Assessment: Procedures for Information System Security Penetration Testing and Rules of Engagement

Distribution:

NODIS

Approved



Marion Meissner
Deputy Chief Information Officer for
Information Technology Security (Acting)

2/11/2011

Date

Change History

Version	Date	Change Description
1.0		Initial Draft
1.1	05/15/09	Restructured document to current SOP format and made minor administrative changes
1.2	02/11/11	Update name, number, and format. Added reference to NPR 2810.1. Changed from ITS-SOP-0017A to ITS HBK-2810.04-02.

Table of Contents

1.0	Introduction.....	5 -
2.0	Purpose.....	5 -
3.0	Scope	5 -
4.0	Roles and Responsibilities	5 -
5.0	Process	6 -
Appendix A: Penetration Test Plan		9 -
Appendix B: Rules of Engagement Template		11 -

1.0 Introduction

A security penetration test is an activity in which a test team (hereafter referred to as "Pen Tester") attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders, the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the target computer in unauthorized ways if it had happened outside the scope of the test. Due to the sensitive nature of the testing, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results.

Applicable Documents

- *NIST SP 800-42, Guideline on Network Security Testing.*
- *NPR 2810.1, Security of Information Technology*

2.0 Purpose

The purpose of this handbook is to layout the procedures and establish the rules of engagement for when security penetration tests are performed against NASA sites (e.g., Centers, facilities, information systems, etc.).

This handbook supports implementation of requirements in *NPR 2810.1, Security of Information Technology*.

3.0 Scope

This handbook applies to all NASA facilities, employees, contractors (as provided by law or contract), recipients of NASA grants and cooperative agreements, partners and visitors, in achieving NASA missions, programs, projects, and institutional requirements.

4.0 Roles and Responsibilities

The NASA Site Point of Contact (POC) shall:

- Be responsible for coordination of the penetration test activities and schedules, and notify management (e.g., Center CIO, IT Security Manager, Security Operations Center (SOC) Manager, etc.) of planned activities.
- Coordinate the penetration test with the NASA Site Point of Contact (POC).
- Be the recipient of all data generated by and related to the ITS Security Penetration test.
- Shall be responsible for ensuring that all data related to the IT Security Penetration test for each site are removed from the Pen Tester's computer(s) by a method approved by the NASA Site POC.

The Pen Test Point of Contact (POC) shall:

- Be responsible for the penetration test team and be the primary interface with the Site POC for all penetration test - activities. -
- Develop the documentation and plans for the penetration test .
- Identify and assign roles to both the Pen Tester's team and the test participants, identify major milestones for the tasks of the Tester's team, identify estimated dates upon which the major milestones will be completed, and indicate the critical path.

- Identify the steps that will be taken to protect the Test Plan, results, and final deliverables
- Coordinate the IT Security Penetration test with the NASA Site POC.
- Assure that all pertinent reports, logs, test results, working papers and data related to the penetration test are being generated and maintained, and are being stored appropriately.

5.0 Process

5.1 Planning for a Penetration Test of a NASA Site

Prior to the start of a penetration test of a NASA site, a NASA Site POC and Pen Tester POC shall be identified. The Site POC will be the individual responsible for coordination of the penetration test activities and schedules, and notify management (e.g., Center CIO, IT Security Manager, SOC Manager, etc.) of planned activities. The Pen Test POC will be responsible for the penetration test team and be the primary interface with the Site POC for all penetration test activities.

The Pen Tester shall develop the documentation and plans for the penetration test (See Appendix A for the Penetration Test Plan Format). As part of this effort, the Pen Tester shall identify and assign roles to both the Pen Tester's team and the test participants, identify major milestones for the tasks of the Tester's team, identify estimated dates upon which the major milestones will be completed, and indicate the critical path. The Pen Tester shall also identify the steps that will be taken to protect the Test Plan, results, and final deliverables.

5.2 Conducting the Penetration Testing

The following tasks shall be performed by the Pen Tester for sites tested:

- a. Introductory Briefing
 - 1) Introduce key players
 - 2) Provide overview of Pen Tester capabilities
 - 3) Explain objectives of the penetration test
 - 4) Review resources, logistics, and schedule requirements (Site POC and Pen Tester POC)
 - 5) Schedule technical and administrative face-to-face meeting(s)

- b. Technical and Administrative Face-to-Face Meeting
 - 1) Conduct introductions and specify meeting objectives
 - 2) Discuss and finalize the Penetration Testing Plan (Appendix A) and the Rules of Engagement (Appendix B)
 - 3) Discuss selection criteria for target Systems with the Site POC and Pen Tester POC
 - 4) Specify tools and applications that will be used to conduct the penetration tests
 - 5) Finalize resources, logistics, and schedule requirements with the Site POC and Pen Tester POC
 - 6) Discuss and review format for final report(s)

- c. Executive In-Briefing
 - 1) Introduce Pen Tester and key penetration testing staff
 - 2) Review objectives of the penetration test
 - 3) Review selected target systems
 - 4) Review plan and schedule for activities
 - 5) Address issues and concerns

Risk Assessment: Procedures for Information System Security Penetration Testing and Rules of Engagement

- 6) The Penetration Testing Plan and Rules of Engagement shall be signed by all parties prior to the start of testing activities
- d. For Review of IT Security Policies, Procedures, Guidance, and Standards
- 1) Plan and schedule
 - 2) Conduct document examinations, process review, and personnel interviews
 - 3) Document findings and prioritize corrective actions with references for NASA policy or requirements, NIST 800 Series Special Publications, and FIPS requirements
 - 4) Brief findings and recommendations, with associated impact statements, to Site POC, CIO, and ITS Manager, as appropriate
- e. For Outsider Penetration Testing
- 1) Plan and schedule
 - 2) Conduct penetration testing with site staff (e.g., reconnaissance, exploitation of vulnerabilities, intrusion, compromise, analysis, and recommendations)
 - 3) When a vulnerability is exploited, provide the Site POC with a "Stop Report." The Pen Tester shall not exploit the system any further unless the Site POC approves
 - 4) Report findings, risk impacts, and recommended corrective actions to the Site POC via daily and weekly reports
- f. For Insider Penetration Testing
- 1) Plan and schedule
 - 2) Conduct penetration testing with site staff (e.g., reconnaissance, exploitation of vulnerabilities, intrusion, compromise, analysis, and recommendations)
 - 3) When a vulnerability is exploited, provide the Site POC with a "Stop Report." The Pen Tester shall not exploit the system any further unless the Site POC approves.
 - 4) Report findings, risk impacts, and recommend corrective actions to the Site POC via daily and weekly reports
 - 5) Conduct technical presentation to site system administrators on test findings, methods, and approaches
- g. For Documentation of Site IT Security Program, Networks, IT Security Services, Firewalls, and other IT Security tools
- 1) Gather data via interviews and site inspections
 - 2) Document operational concepts of IT security services and control measures
 - 3) Identify all NASA and non-NASA entities with network access or dependencies
 - 4) Summarize findings identifying weaknesses and strengths. Each weakness shall be referenced to a NASA or government requirement
 - 5) Conduct working session with key players
 - 6) Recommend corrective actions and prioritize them based on cost/benefit model
- h. Analysis of Data and Findings (off-site)
- 1) Correlate data and findings from discoveries and reviews
 - 2) Analyze results from penetration testing
 - 3) Compare requirements with NASA or government requirements
 - 4) Document findings and prioritize recommended corrective actions with references to NASA or government requirements
 - 5) Provide briefing of findings, recommendations, and associated impacts, to Site POC, CIO, and ITS Manager
 - 6) Review draft reports with Site POC

i. Exit-Briefing

- 1) Summarize findings
- 2) Present final reports
- 3) Discuss outsider penetration testing results
- 4) Discuss insider penetration testing results
- 5) Discuss evaluation of Site's IT security program and management structure
- 6) Discuss overall recommendations

5.3 The Pen Tester shall remove all data related to the IT Security Penetration test for each site from the Pen Tester's computer(s) by a method approved by the NASA Site POC. All documents, data logs/files, test results, and working papers generated by the Pen Tester for the IT Security Penetration test at each site shall not be retained by the Pen Tester and shall be provided to NASA, become the property of NASA, and be retained by the respective NASA Site POC.

Appendix A: Penetration Test Plan

I. Planning and Enumeration

Provide a short narrative discussion of the activities associated with each of the following,

- Identify Scope and Goals of the Exercise
- Enumerate the Boundary of the Testing
- Develop Rules of Engagement
 - Conduct penetration testing with site staff (e.g., reconnaissance, exploitation of vulnerabilities, intrusion, compromise, analysis and recommendations)
 - When a vulnerability is exploited, describe the actions to be taken such as: issuing a "Stop Report" stopping further exploiting the system unless the approved
 - How findings, risk impacts, and recommended corrective actions will be reported: such; daily and weekly reports unless high risk which will be report immediately
 - Conduct technical presentation to site system administrators on test findings, methods, and approaches

2. Vulnerability Analysis

Provide a short narrative discussion of the activities associated with each of the following included in the penetration testing.

- Identify Targets
- Identify Potential Vulnerabilities
- Perform Vulnerability Scans
- Buffer overflows
- Improperly configured network services
- Improperly configured trust relationships
- Insecure authentication mechanisms
- Outdated network services that have known vulnerabilities
- Apply enumeration data in searching vulnerable databases
- Perform manual tests
- Password guessing
- IP spoofing
- Social engineering
- Manipulating routing tables
- Identification and usage of modems and wireless access points as an attack vector for entry into the NASA network.

3. Penetration Testing

Provide a short narrative discussion of the activities associated with each of the following.

- Research and develop attack scenarios
- Execute attacks

- Record results
- Report exploitable vulnerabilities
- Analyze penetration testing results and if indicated, perform additional exercises
- Recommend countermeasures

Penetration Testing Project Manager Site

IT Security Manager (ITSM) or CIO

Appendix B: Rules of Engagement Template

Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of *[required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

Penetration Test Purpose

The purpose is to assess the vulnerability of the NASA *[target system or capability]* and supporting Information Technology infrastructure regarding unauthorized access from outside and inside of NASA. The procedures are designed to be non-intrusive and are intended to validate security configuration controls that protect systems that are relevant to our *[target, e.g., financial statement audit, IT security]*. The purpose of this effort is to satisfy audit requirements under *[cite requirement, e.g. the Chief Financial Officer's Act, Federal Information Security Management Act, etc.]* for testing of internal controls involving computer-based systems and data communications networks. This methodology will be used as stipulated in the *[Statement of Work, Task order]* to help provide an understanding of risks, internal controls, and vulnerabilities in networked computing environment supporting NASA's data and its operation.

Penetration Test Objective

The objectives of the testing are to:

- Evaluate the protection of NASA information technology assets (i.e., data, systems, and processes), with a special emphasis on the effectiveness of logical access and system software controls
- Provide value to the Agency's *[program being tested, e.g., financial management program, IT Security, etc.]* and the auditee by identifying opportunities to significantly strengthen applicable controls within budgetary and operational constraints

To facilitate timely, cost-effective completion of this project, *[third party]* will make maximum practical use of the relevant work of others (e.g., internal assessments by the auditee, internal and external audits, and vulnerability testing on covered IT assets).

Scope

[Third party's] penetration procedures will be designed to remotely (via internet, wireless, and dial-up) as well as locally (within NASA's facilities) scan the application, database and web servers supporting NASA as well as any other IT infrastructure components deemed critical in supporting NASA's operating environment. Penetration procedures will only be conducted against applications, databases, web servers, and IT infrastructure jointly identified by *[third party]* and NASA and approved by the Center CIO.

The external penetration testing will be performed from *[third party's]* facility and location, and/or other secured facility external to NASA network infrastructure and the internal penetration testing will be performed at *[location, e.g., Center, Installation]*.

[Third party's] test procedures will use non-destructive testing techniques (i.e., no files or data on the target systems are to be modified, added, deleted, or changed). Evidence to support any access control weaknesses discovered should consist primarily of screen prints and session logs.

Timing

The external penetration testing will be performed during the week of *[date and year]*, specifically on *[month, days]* followed by internal penetration testing during the week of *[date and year]* specifically on *[month, days]*. The actual date and time of the initiation of these procedures will be mutually defined and agreed upon by *[third party]*, and *[appropriate NASA management officials]*, NASA IT management, and the Center CIO.

Methodology

[Third party] plans to conduct this vulnerability assessment in four phases:

1. **Planning the scope of assessment:** *[Third party]* team will hold discussions with *[NASA or Name o/Center]* management to finalize the scope of assessment. *[Center or installation]* IT management will provide
 - a. The range of IP addresses to be scanned during both the external and internal assessment
 - b. The range of phone numbers to tested during war-dialing exercise
 - c. The area in which war-driving will be permitted.

Internal analyses and tests of password policies and their implementation (Level 1). These steps are designed primarily to identify the potential for unauthorized and/or inappropriate access to systems on the auditee's network.

"Outside-in" security testing of computer systems and networks (Level 2). These steps are designed to identify vulnerability of the auditee's network and IT infrastructure to outside hacking. They include: searching for publicly available sources of information about the auditee's network, use of automated dialing tools to check for accessibility of modems and connected host computers within the auditee's infrastructure, and external testing for vulnerabilities through a defined subset of the auditee's Internet points of presence.

Coordinated internal and external systems and network vulnerability assessments and testing (Level 3). These steps are designed to identify the vulnerability of NASA's IT assets to fraud or malicious attacks by knowledgeable insiders, working alone or in concert with knowledgeable outsiders. These steps are intended to identify the potential effects of vulnerabilities arising from security deficiencies found in perimeter network defense or internal network or host computer security configuration.

[Third party! will require [number! designated representatives from [appropriate NASA organizations! to be present and/or readily available (via phone) during portions of the vulnerability testing attempts.

ASSESSMENT TOOLS

External/Internal Testing Tools

[Third party] will be using the [identify scanning tool to be used] remote security scanner while performing the external and internal testing portions of the vulnerability assessment. [Provide a description of the scanning tool and a description of its capabilities or attributes]. Additional information on [scanning tool] can be found at [url for additional information on scanning tool].

War Dialing/Driving Testing Tools

[Third party] will be using [name of war-dialing tool] while performing the war-dialing portion of the vulnerability assessment. [Description of the war-dialing tool and a description of its capabilities or attributes]. Additional information on [war-dialing tool] can be found at [url for additional information on scanning tool].

[Third party] will be using [name of war-driving tool] while performing the war-driving portion of the vulnerability assessment. [Description of the war-driving tool and a description of its capabilities or attributes]. Additional information on [war-driving tool] can be found at [url for additional information on scanning tool].

Wireless Testing Tools

[Third party] will be using [name of wireless testing tool] while performing the wireless testing portion of the vulnerability assessment. [Description of the wireless testing tool and a description of its capabilities or attributes]. Additional information on [wireless testing tool] can be found at [url for additional information on scanning tool].

RULES TO BE FOLLOWED

The following are agreed upon rules that will be followed as part of this penetration test:

- Designated NASA and *[other functional]* representatives will observe and/or be readily available to discuss while in progress all *[third party]* penetration/exploitation activity with the exception of initial war dialing to obtain the list of numbers with attached modems
- Penetrations into NASA systems will only be pursued insofar as they could lead to access to significant *[type of systems, e.g. financial, program]* systems or are significant to the entity-wide security program of the overall network environment at NASA. If testers are detected and blocked, then the appropriate *[functional representatives]* and CIO contacts will be notified and the block will be acknowledged and released
- Under no circumstances will a network or system compromise at NASA be exploited that results in the penetration of one or more of NASA's corporate or government partners'
- Prior to any war dialing efforts, a "Do Not Call" list will be provided to the *[Third party]* Penetration team. The team shall configure their environment to strictly adhere to this "Do Not Call" list
- All passwords compromised during testing will be reported to the designated *[functional representatives]* and the CIO contact for resetting.
- All *[Third party]* reports and work papers will be clearly labeled "Limited Distribution Confidential and Proprietary NASA Information".
- *[Third party]* will not issue the results of its penetration testing to the *[interested NASA officials]* via unencrypted e-mail.
- *[Third party]* will ensure penetration testers have at least a U.S. SECRET clearance. Clearances will be coordinated with *[Center or Installation's]* physical security office at least 10 working days in advance.
- External penetration testing will be performed from a secured facility (external to NASA) and internal penetration testing will be performed at *[Name of Center or Installation]*. *[Third party]* will not perform this exercise at any other location.
- Prior to connecting to the NASA network, all non-NASA computer equipment used to perform the internal assessment will be running anti-virus software with the latest updated signature files. *[Name of Center or Installation's]* IT security staff, using normal procedures, will scan the all non-NASA systems for vulnerabilities and *[Third party]* will make necessary corrections. Additionally, this equipment will also have installed the latest operating system and application service packs and patches.
- Prior to connecting to the NASA internal network, NASA, with the assistance from *[Third party]* and *[other interested NASA functions]* will examine all non-NASA computer equipment used to perform the internal assessment to ensure that no new threats are introduced to the NASA internal network by non-NASA equipment. This will include verification of the existence and/or proper functionality of anti-virus software and operating system with application service packs and patches
- All network scanning procedures will be accomplished within the specified time mutually agreed upon by *[Third party]*, the *[functional representative]*, and NASA management.
- A full network scan will not be performed. A targeted network scan will be completed and limited to the subnets and targeted hosts, so as to control and further minimize load on the network infrastructure. Configurations of the boundary/edged routers at the points of interface of these systems with the rest of the NASA network will be checked, however. *[Third party]* will refrain from any denial-of-service attempts.

- In its penetration efforts, *[Third party]* will at **no point exploit** identified vulnerabilities. Accordingly, no files and directories will be altered or deleted. *[Third party]* will run non-destructive procedures to verify level of permissions associated with logon accounts and identify network addresses accessible from NASA systems where access controls were circumvented. No updates will be made to data files
- No non-NASA files or programs are to be left on any of NASA's computer resources. All files, data, and programs installed or loaded on to NASA systems will be documented and removed at the conclusion of the test
- User files and any other data contained with any information system resources that are part of an agency system of records on individuals to which *[Third party]* obtains access will be kept confidential in a manner consistent with the Privacy Act (5 U.S.C. §552a) and the applicable agency regulation (45 C.F.R. part 613).
- Utmost care will be exercised not to disable user IDs for any extended period of time. For any user ID found to be inadvertently disabled, we will notify the NASA test monitor and/or appropriate engagement coordinator to enable the prompt restoration of access.
- Any procedures that have potential negative impact on network traffic or interruption will be avoided. Where necessary to demonstrate to NASA the full nature and extent of a vulnerability, such procedure will either be performed during off-peak hours or will be demonstrated on a NASA test system configured to simulate the live network environment.

Notification Procedures

An appointed NASA designee as well as a representative from the *[functional representative]* will observe and/or review *[Third party's]* activities to validate that testing is performed in accordance with this Rules of Engagement. Each Center Information Technology Security Manger will be kept apprised of the timeline and extent of the penetration testing being done at their Center. The numbers for the key contacts are included within the Point of Contact table.

Information to Be Provided by Client

As part of maximizing the value of this test and to minimize any potential disruption to operation, we request the following information to be provided upon authorization to proceed:

- Listing of all IP addresses for the defined targets (application, web server, database) within the scope of this test.
- A complete list of phone numbers/analog line ranges identified by NASA.

Reporting

The results of this IT Penetration test will be presented only to NASA and the *[Functional representative]* in a memorandum detailing the procedures performed and observations noted during this penetration test. All information about this engagement, the information systems vulnerabilities and potential security compromises will be kept confidential by *[Third party]*. Upon completion and acceptance by the OIG, all media, records,

documents, notes, and files, **except for the documentation retained by [Third party] for its working papers**, shall be turned over to the OIG.

Points of Contact

Organization	POC Name	Number/E mail Address
<i>[Third party]</i>	<i>Name</i>	Voice: Mobile: e-Mail:
	<i>Name</i>	Voice: Mobile: e-Mail:
<i>[Functional Area]</i>	<i>Name</i>	Voice: e-Mail:
	<i>Name</i>	Voice: e-Mail:
NASA	<i>Name</i>	Voice: e-Mail:
	<i>Name</i>	Voice: e-Mail:

Authorization to Proceed

The following parties have acknowledged and agree to the test objectives, scope, rules to be followed, information to be provided, and the notification procedures. Signature below constitutes authorization to *[Third party]* to commence with the penetration test described above.

Deputy Chief Information Officer for
Information Technology Security
Office of the Chief Information Officer
National Aeronautics and Space
Administration

Date

[Name of Functional Rep.]

[Title]

National Aeronautics and Space
Administration

Date

[Name of Functional Rep.]

[Title]

Office of the Administrator
National Aeronautics and Space
Administration

Date

[Name of Center Representative]

[Title]

Office of the Chief Information Officer

Date

[Center Name]

National Aeronautics and Space Administration

[Name]

Principal

[Third Party's Organization]

Date

[Name of Third Party]