



Network Security Assessment Test Plan

for

Savoy06 has been contracted by [Name of client] to perform an audit of client's IT network which requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having these "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.

Limited Distribution

Confidential and Proprietary

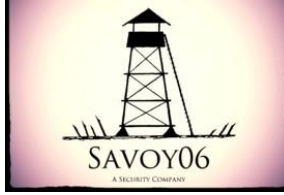
All rights reserved Savoy06, 2018

No part of this publication may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Savoy06.



Table of Contents

Points of Contact.....	3
Test objectives.....	4
Scope.....	4
Information to be provided by client.....	4
Rules of Engagement.....	5
Authorization to Proceed.....	6



Points of Contact

Point of contact for client

Phone

Point of contact for Savoy06

Phone

Escalation point of contact for Savoy06

Phone



Test objectives

- Evaluate the protection of client information technology assets with a special emphasis on the effectiveness of logical access and system software controls.
- Provide value to the client's program being tested by identifying opportunities to significantly strengthen applicable controls within budgetary and operational constraints.

Scope

Savoy06's penetration procedures will be designed to remotely (via internet, wireless, etc) as well as locally (within client's facilities) scan the application, database and web servers supporting client as well as any other IT infrastructure components deemed critical in supporting client's operating environment. Penetration procedures will only be conducted against applications, databases, web servers, and IT infrastructure jointly identified by Savoy06 and client.

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].

Information to be provided by client

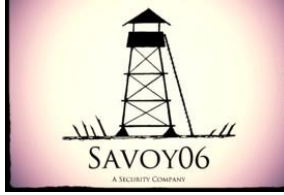
As part of maximizing the value of this test and to minimize any potential disruption to operations, we request the following information to be provided upon authorization to proceed:

Listing of all IP addresses for the defined targets (application, web server, database) within the scope of this assessment:



Rules of Engagement

- Designated client will be readily available to discuss while in progress all Savoy06 penetration/exploitation activity.
- Penetrations into client systems will only be pursued insofar as they could lead to access to significant systems or are significant to the entity-wide security program of the overall network environment at client.
- Under no circumstances will a network or system compromise at client be exploited that results in the penetration of one or more of client's corporate or government partners
- All passwords compromised during testing will be reported to the PoC for resetting.
- Savoy06 will not issue the results of its penetration testing to the client via unencrypted e-mail.
- External penetration testing will be performed from a remote facility (external to client) and internal penetration testing will be performed at client's location.
- Prior to connecting to the client local network, all non-client computer equipment used to perform the internal assessment will be running a Savoy06 approved OS image.
- All network scanning procedures will be accomplished within the specified time mutually agreed upon by Savoy06 and the client PoC.
- Savoy06 will refrain from any denial-of-service attempts.
- In its penetration efforts, Savoy06 will at no point exploit identified vulnerabilities. Savoy06 will use non-destructive procedures to verify level of permissions associated with logon accounts and identify network addresses accessible from client systems where access controls were circumvented.
- No non-client files or programs are to be left on any of client's computer resources.
- User files and any other data to which Savoy06 obtains access will be kept confidential.
- For any user ID found to be inadvertently disabled, Savoy06 will notify the client to enable the restoration of access.
- Any procedures that have potential negative impact on network traffic or interruption will be avoided. Where necessary to demonstrate to client the full nature and extent of a vulnerability, such procedure will either be performed during off-peak hours or will be demonstrated on a client test system configured to simulate the live network environment.



Authorization to Proceed

The following parties have acknowledged and agreed to the objectives, scope, and rules of engagement as described in this Test Plan. Signature below constitutes authorization to Savoy06 to commence with the assessment.

_____	_____	_____
Point of contact for client	Date	Phone

_____	_____	_____
Point of contact for Savoy06	Date	Phone