



# VoIPshield VoIP/UC Penetration Testing Services

## SERVICE DESCRIPTION

Date: **December 2008**



## Table of Contents

1	INTRODUCTION.....	2
2	BACKGROUND .....	2
3	VALUE PROPOSITION.....	2
4	SERVICE DESCRIPTION .....	2
5	ASSUMPTIONS.....	5
6	DELIVERABLES .....	5
7	COST .....	5



## 1 Introduction

VoIPshield Systems Inc. ("VoIPshield"), the global leader in VoIP security, researches threats and vulnerabilities associated with common VoIP protocols and devices from major vendors. Our world-class team of security researchers developed highly effective penetrations techniques and tools that enable us to quickly assess and identify security problems related to VoIP/UC systems deployed by enterprises.

## 2 Background

The VoIPshield security service offering for vendors includes penetration testing services for VoIP and UC installations

Penetration testing services offer multi-dimensional analysis of VoIP/UC security infrastructure including protocols, access interfaces, protocol fuzzing, DoS and many others.

## 3 Value Proposition

VoIP/UC penetration testing helps protect the enterprise from security risks and attacks that can cause:

- Financial loss through toll fraud or through lost revenue due to unreliable VoIP/UC systems and processes.
- Non-compliance with industry regulations.
- Impact on the brand and loss of consumer confidence and business reputation.
- Un-patched vulnerabilities that could lead to security attacks and exploits resulting in financial losses.

## 4 Service Description

VoIPshield will commence work with a kick-off meeting between VoIPshield and all appropriate Client stakeholders to review the scope of the engagement and get agreement on the assumptions and objectives of the project.

Meeting minutes will be generated and provided to the Client for verification and approval.

VoIPshield will request all relevant documentation from the Client for review.



The VoIPshield penetration testing methodology consists of the following major steps:

- 1 Planning and information gathering
- 2 Enumeration and scanning
- 3 Vulnerabilities identification and verification
- 4 Vulnerability exploitation and penetration
- 5 Findings verification
- 6 Report and Presentation

1. Planning stage sets the objectives and defines attacker profiles:

- Pen test approach: remote/local, eternal/internal, black box/white box, etc.
- Decide if exploits will be performed and to what extent.
- Define success criteria with which organization can measure results.
- Interface to IT and telecommunication organizations are defined.
- Obtain management approval for the pen test.
- Project duration defined.

2. Information collection

- Identification of network and devices access points.
- Packet flow diagrams
- Network mapping, port scanning and application fingerprinting
- Public information on the owner of the network or application in question to plan a comprehensive attack.

3. Identify and Verify vulnerabilities

- Authorized attacks using public, custom, and professional tools to search for vulnerabilities in the targets, which will allow access permission.



- Compile a list of compromised hosts for the next stages.
- Designing and planning exploits.

#### 4. Vulnerability exploitation

- Based on analysis of vulnerabilities identified in Step 3 the pen testers perform the attacks.
- The attack escalation based on compromised VoIP/UC devices used as points to perform attacks on other components of VoIP/UC networks.
- The iterative process is continued until defined objectives are achieved.

#### 5. Findings Verification

- The results of the pen tests are verified to minimize false negatives.

#### 6. Report and Presentation

A report will be generated after the pen testing is concluded. The report will consist of the following section headings:

- Executive Summary
- Introduction
  - Description of pen testing process
  - VoIPshield team composition
  - Date, time, location of assessment activities
- Objectives
- Methodology detail
- Significant Observations
- Findings
- Recommendations
- Appendix
  - Detailed results of all testing, including log files, etc.



VoIPshield will provide this report to the Client and schedule a meeting to present the findings and discuss the report in detail. This meeting may be done in person or through teleconference, as requested by the Client.

## 5 Assumptions

- Client is aware of potential impacts and accepts the risks associated with device and application pen testing testing.
- Client has clear and documented authority to sanction scanning work associated with device and application testing.
- Client will respond to all VoIPshield inquires, and sign-off on all procedural and management documentation, within 2 working days.
- Client has established lines of communication and notification regarding system help and problem resolution.

## 6 Deliverables

- Documentation around meetings and decision points
- Draft Pen Testing Results report and recommendations
- Final Pen Testing Results report and recommendations. This is a detailed report including a list of priority/severity results, recommendations, and an appendix of all tests conducted showing the corresponding results.
- Final presentation

## 7 Cost

Please contact VoIPshield for more details.