



VoIP Security Services Technical Description

Cyber 51 LTD.

DOCUMENT CLASSIFICATION:

PUBLIC

Copyrighted Material

No part of this publication, in whole or in part, 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 distance learning, in any form or by any means such as any information storage, transmission, or retrieval system, without prior written permission from the author.



Table of Contents

VOIP PENETRATION TEST.....	3
INTRODUCTION.....	3
METHODOLOGY.....	3
<i>Reconnaissance</i>	3
Footprinting.....	3
Scanning.....	3
Enumerating.....	4
<i>Vulnerability Analysis</i>	4
<i>Exploiting</i>	4
<i>Reporting</i>	5



VoIP Penetration Test

Introduction

Voice over IP (VoIP) is being rapidly embraced across most markets as an alternative to the traditional public-switched telephone network. VoIP is a broad term, describing many different types of applications and using a wide variety of both proprietary and open protocols that depend heavily on your preexisting data network's infrastructure and services.

Because VoIP packetizes phone calls through the same routes used by traditional enterprise data networks today, it is consequently prone to the very same cyber threats that plague those same networks. These include denial-of service attacks, worms, viruses, and general hacker exploitation.

For instance, if your enterprise is under attack from a distributed denial of service (DDoS) attack, internal users' web browsing might be slower than normal, but *a DDoS attack on a VoIP-enabled network can completely cripple your VoIP applications, at least to the point where conversations are unintelligible.*

Our VoIP penetration test service points to follow same activities as a malicious hacker in order to verify and find weaknesses in your VoIP deployments, reporting every vulnerability indicating associated risks and helping you to elaborate a detailed remediation plan.

Methodology

Reconnaissance

The first phase of our services will focus in demonstrating how an attacker would first scan the whole network and then pick up specific targets and enumerate them with great precision in order to proceed with further advanced attacks through or from the hacked VoIP devices. In order to do that, we are going to follow the below steps:

Footprinting

In this stage, we will elaborate a profile about the target organization by performing passive reconnaissance using tools such as Google, DNS, and WHOIS records, as well as the target's own website.

Scanning

In this stage, we are going to use different remote scanning techniques in order to identify potentially active VoIP devices on the network. We cover the traditional UDP, TCP, SNMP, and ICMP scanning techniques as applied to VoIP devices.



Enumerating

In this stage, we will be performing various active methods of enumeration over the different detected VoIP devices, from softphones, hard phones, proxies, and other general SIP-enabled devices.

Vulnerability Analysis

After successfully identifying the target systems and gathering the required details from the above phases, a penetration tester will try to find any possible vulnerabilities existing in each target system.

During this phase a penetration tester will use automated tools to scan the target systems for known vulnerabilities. These tools have their own databases consisting of latest vulnerabilities and their details.

Exploiting

In this phase, once we have all the recollected information gathered on previous phases of the service, we are going to perform different exploitation tasks targeting the network infrastructure on which your VoIP applications depend.

Most of the techniques are originated from the traditional data security world, but applied here against VoIP devices and supporting network services.

Also, for this specific stage, we have many open source and commercial tools in place that help us in the different exploitation tasks (for example, CANVAS and a VoIP exploitation pack)

Some techniques and tests:

- VoIP Network Infrastructure Denial of Service (DoS)
- VoIP Network Eavesdropping
- VoIP Interception and Modification
- VoIP Session and Application Hacking
- Fuzzing VoIP
- Flood-Based Disruption of Service
- Signaling and Media Manipulation

Note 1: DoS and DDoS are only tested if they have been accepted as solicited at Project's scope definition.

Note 2: Eavesdropping and Interception techniques are only used in onsite test procedures.



Reporting

The last phase in the entire activity is the reporting phase. This phase can occur in parallel to the other three stages or at the end of the Attack stage.

The final report will be prepared keeping in mind both Management as well as Technical aspects, detailing all the findings with proper graphs, figures, etc. so as to convey a proper presentation of the vulnerabilities and it's impact to the business of the target organization.

An executive summary, describing in brief, the activities performed, findings, and high-level recommendations will be provided.

Also detailed technical descriptions of the vulnerabilities and the recommendations to mitigate them will be documented in this report. All the security holes found and exploited will be accompanied with proper Proof-of-Concept by means of screenshots of the successful exploits, or any other such methods.

This report will consist in an Executive report containing, without to be limited to: conclusions, recommendations, statistics, and hacking methodology brief, and a Technical Report containing without to be limited to: Information Gathering, Network Information, Analysis and Attack results of accomplished tasks.