



Think Your VoIP is Secure? Think Again.

VoIPshield Systems is the leading provider of security products designed specifically for VoIP.



Vulnerability assessment and penetration testing for VoIP networks

VoIPaudit™ 2.0

VoIPshield Systems Inc
150 Katimavik Road, Unit 102
Ottawa, Ontario
Canada K2L 2N2

Telephone: 613.591.6589

info@voipshield.com

VoIPaudit is the only vulnerability assessment and penetration testing product available that is specifically designed to identify Voice over IP (VoIP) vulnerabilities in enterprise VoIP systems.

VoIPaudit is a VoIP network scanning tool that offers an easy-to-use Web interface combined with all the back-end functionality required to proactively identify, track and assist in the remediation of security vulnerabilities found in VoIP systems from the leading vendors.

Features include:

- VoIP network discovery
- Network scanning for security vulnerabilities and threats
- Optional penetration testing
- Asset management
- Comprehensive reporting including detailed explanation of potential threats and remediation suggestions

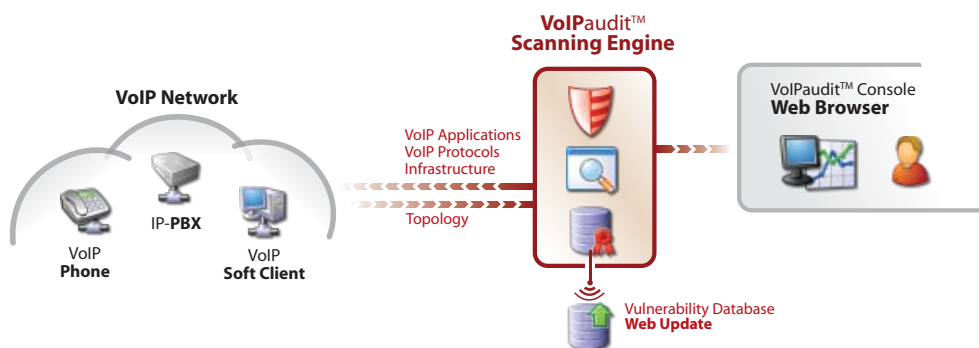
Traditional data security products are not equipped to identify or protect against the unique vulnerabilities and exploits associated with VoIP systems. The "real-time" nature of voice traffic, combined with new protocols, hardware and applications, require security products that are purpose-built for VoIP. VoIPaudit combines familiar approaches to vulnerability assessment (VA), such as full-network scanning and asset discovery and management, with a proprietary database of thousands of VoIP-specific test cases, to produce a result that traditional VA tools simply can not match.

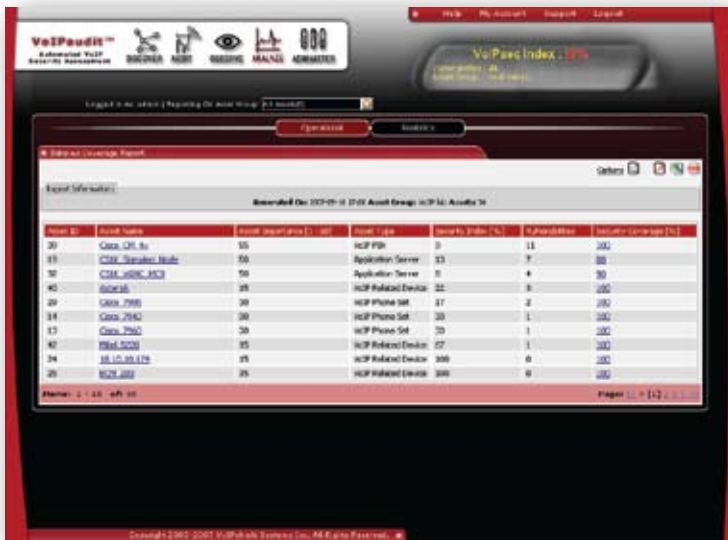
VoIPaudit allows your organization to:

- Keep VoIP quality of service, reliability and security at levels comparable to existing circuit-switched voice;
- Identify potential denial of service, confidentiality, toll fraud and voicemail vulnerabilities before they are exploited;
- Assure VoIP implementation compliance with internal and government regulations.

Like vulnerability assessment and penetration testing tools from the data world, VoIPaudit 2.0 automatically scans the entire VoIP network, looking for security vulnerabilities that could compromise the availability and integrity of not only your voice system, but in unified environments, your data assets as well. For each vulnerability found, the system identifies corresponding remedial action that should be taken to mitigate the risks. The vulnerabilities and exploits database is continually updated via VoIPaudit's ActiveUpdate™ mechanism, so as new threats are discovered the system automatically tests for them.

Included in the VoIPaudit license is a one-year subscription to VoIPshield Update™, which provides ongoing software upgrades and vulnerabilities updates. VoIPshield Laboratories, the research division of VoIPshield Systems, is constantly discovering new vulnerabilities and adding them to our database. This means VoIPaudit is always able to detect the most recently-discovered vulnerabilities.





With VoIPaudit, security and IT staff can reduce or eliminate error-ridden manual checks and perform efficient assessments of their VoIP infrastructure without the need for specialized training.

Benefits

VoIPaudit offers enterprises and security consultants these benefits:

- **Complete Coverage.** The only commercially available VoIP vulnerability assessment and penetration testing tool to support both standard (SIP, H.323, RTP) and proprietary (Skinny, UNISTIM) based VoIP solutions.
- **Industry Leading Research.** The industry's most extensive database of VoIP-specific vulnerabilities and threats constantly updated by world-class VoIP security research team.
- **Highly Mobile.** VoIPaudit moves seamlessly between networks, sites and branches without the need for system reconfiguration.
- **Fast Results.** VoIPaudit deploys in minutes and users can immediately run a set of pre-defined "most common" audits for out-of-the-box usability.
- **Ease of Use.** A Web-based user interface provides familiar access to all functions.
- **Reporting.** Standard and custom reports provide operational and analytical information to executives, managers and technical personnel.

Technical Specs:

Server Appliance Version:

- 2.0 Ghz Dual Core Xeon CPU x2
- 4Gb of Ram
- 73Gb 15000RPM Hard disk
- Red Hat ES 4.0
- Min. Single Network Interface Card (NIC)

Laptop Appliance Version:

- 2.0 Ghz Dual Core CPU
- 2Gb of Ram
- 80Gb Hard Disk
- Red Hat ES 4.

VoIP Network Discovery and Asset Management

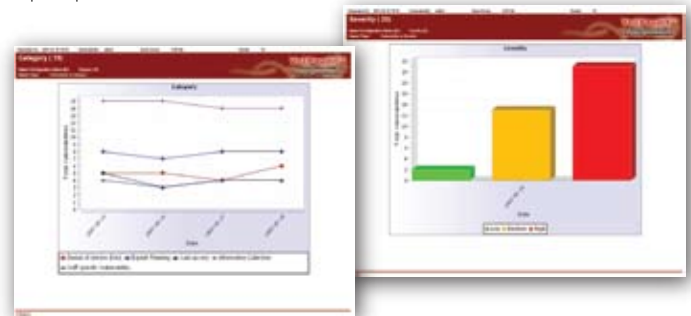
- In-depth discovery of VoIP infrastructure assets including PBXs, softswitches, gateways, multi-media servers, phones and soft clients. VoIPaudit's discovery process is fast, with low impact.
- Comprehensive asset management system tracks changes to the VoIP infrastructure.
- Discover and manage multiple VoIP networks simultaneously. System administrator can seamlessly switch between VoIP networks, sites, or branches without re-configuration.

VoIP Network Vulnerability Audit

- Comprehensive set of pre-defined audits is provided out-of-the-box to "quick-start" the scanning process.
- Configuration wizards enable custom audit definitions, allowing for more targeted reporting and system optimization. Audit definitions are stored in the database and are available to users based on their roles.
- Run-time selection of non-destructive and/or destructive test cases. Users can select various port scanners and configure special test cases that require authentication parameters. Select all or specific targets and test cases.
- Test cases derived from the industry's most comprehensive database of VoIP vulnerabilities and exploits.
- Receive database updates automatically or manually through "VoIPshield Update" mechanism.

VoIPaudit Reporting

- Detailed technical reports show vulnerability descriptions and indicate potential impact on VoIP devices if/when exploited.
- Detailed remediation instructions are provided for each vulnerability found.
- Coverage reports show which test cases were executed.
- Executive level reports provide summary information in "scorecard" format and graphically depict trending information.
- Export reports to PDF, CSV and XML formats.



System Administration and Management

- Web-based interface allows authorized access from any location.
- Role-based user access controls.
- "Group" functionality assigns responsibilities based on target type and associated test cases.
- Software upgrades and updates to the vulnerabilities database controlled by the user.
- Appliance-based or software-based product distribution.