



[ VULNIT ]  
Vulnerability  
Identification Tool

# VulnIT

## Technical documentation



# Introduction

VulnIT provides a suite of 3 products embedding our software:

- a bootable USB key, shipped with the whole environment required to perform your security testing without any installation,
- the virtual machine automates IT security monitoring,
- the SaaS solution available on our website enables on-demand testing for an effective assessment of the organization's out-facing security.

The technical tests performed by our software are described below.

## Tests list

### *Network port scanning*

The first acquisition step consists in detecting all the devices reachable in the audit scope provided (target acquisition) and detecting all the services provided by each target (service identification).

The TCP scanner used is [synscan](#). It is a TCP SYN (half open) scanner.

The test depth selected is:

- fast (only the 100 most used ports will be tested),
- normal (the 1000 most used ports will be tested) or
- full (all 65535 ports will be tested).

A SNMP (UDP) scan is also performed using [medusa](#), on a selection of a few common community strings. The SNMP service is the only UDP service scanned at the moment.

### *Domain discovery (specific to VulnIT-SaaS)*

VulnIT-SaaS intends to discover all the assets belonging to a (using DNS, Google, RIR and SPF).

Besides, VulnIT-SaaS discovers the following vulnerabilities on the domain or the assets belonging to the domain without testing the assets themselves:

- List of all the vulnerable pages identified by Google and Bing,
- Black-listed domain, blocked by anti-spam softwares (DNS-based Block List),
- Websites containing malwares (Google safe-browsing),
- Documents containing meta-data (user name, etc).

## ***Vulnerability assessment***

The testing phase performs adequate vulnerability assessments, depending on the targets and services selected during the validation step (see the user guide above).

These tests concern the following criteria:

- Patch management,
- Development,
- Access control,
- Configuration,
- Encryption,

On a panel of technologies:

- Windows and Unix systems,
- Websites,
- Networks
- Databases.

	<b>Patch mgt</b>	<b>Develop-ment</b>	<b>Access control</b>	<b>Configuration</b>	<b>Encryption</b>
<b>Windows (OS and apps)</b>	✓			✓	
<b>Unix (OS and apps)</b>	✓			✓	
<b>Websites</b>	✓	✓	✓	✓	✓
<b>Databases</b>	✓		✓	✓	
<b>Networks</b>	✓		✓	✓	✓

These tests are detailed hereunder.

### **Websites testing**

All websites (Internet, Intranet, Extranet) are first discovered. This crawling phase enumerates all the accessible web pages of the website, either they are naturally linked (HTML links, Javascript, Flash banners) or hidden (dictionary-based approach).

Once these pages enumerated, VulnIT automates the identification of the following development vulnerabilities:

- SQL injection (blind SQLi, supporting 4 technologies of underlying databases: Oracle, SQL Server, MySQL and PostgreSQL),

- XSS (Cross-site scripting),
- File inclusion, either local (LFI) or remote (RFI),
- CSRF (Cross-Site Request Forgery),
- Session management,
- Unvalidated redirect,
- Trivial authentication vulnerabilities (in web forms or http .htaccess security).

The OWASP classifies these vulnerabilities as the most critical and also the most frequent vulnerabilities on websites.

VulnIT also detects misconfigurations which could lead to information leakage:

- Temporary files (development or backup files),
- FPD (Full Path Disclosure) indicating the web server architecture,
- The TRACE function activated on the web server,
- Detecting the web server version.

## **Patch management**

Patch management is tested using [OpenVAS](#), which runs a collection of plugins dedicated for each patch to check.

On November 2010, about 8200 plugins are included in our tests and cover the following flavors of operating systems:

- CentOS,
- Debian,
- Fedora,
- FreeBSD,
- Gentoo,
- HP-UX,
- MAC OS-X,
- Mandrake,
- RedHat,
- Solaris,
- Suse,
- Ubuntu,
- Windows (security bulletins and advisories)

And also databases and web servers.

In order to avoid affecting the target availability, we excluded 'aggressive' plugins on the following criteria: the plugin is explicitly described as aggressive, it attempts brute forcing, or it falls into one of the 'aggressive' categories ('ACT\_DENIAL', 'ACT\_DESTRUCTIVE\_ATTACK', 'ACT\_FLOOD', 'ACT\_KILL\_HOST' or 'ACT\_MIXED\_ATTACK', as described in [NASL documentation](#)).

We also excluded the plugins raising low and medium risk issues, i.e. which [CVSS](#) (Common Vulnerability Scoring System) is between 0 and 7, mostly because we only

focus on high-risk issues. Besides, they tend to be unreliable and requiring a lot more time to process.

## **File shares**

Dedicated tests are performed on file shares:

- Anonymous access on FTP servers,
- Windows folders shares (or samba shares on Unix) open to everyone.

## **Databases**

Authentication tests (for trivial accounts) are performed on 5 technologies of database management systems:

- Microsoft SQL Server,
- Oracle,
- MySQL
- PostgreSQL,
- DB2 (Unix/Windows).

## **Wifi console**

A wifi console providing information on the access points accessible: SSID (name), power, channel, and security settings (open, WEP, WPA).

We do not offer the ability to crack a WEP password for instance.

## **Network security**

A few common network security checks are performed:

- SSH authentication tests (using a dictionary of trivial accounts),
- Read/write SNMP access using common community strings,
- Open mail relay (attempting to send 10 unauthenticated emails),
- Microsoft RPC information leakage,
- SSL null or weak ciphers allowed,
- DNS zone transfer,
- Unencrypted protocols (Telnet, Rexec/Rsh/Rlogin, FTP)

# VulnIT

## Technical documentation:

[www.vulnit.com/support.php](http://www.vulnit.com/support.php)

[www.vulnit.com/ressources.php](http://www.vulnit.com/ressources.php)

## Contact:

[www.vulnit.com/contact.php](http://www.vulnit.com/contact.php)

The information provided on this document are based on the technical characteristics at the moment of its production.

As part of the constant improvement of our products, VulnIT may change the information provided in this document at any time.

All the pictures, images and texts used on this document are copyrighted by VulnIT. Any copy, even partial, is not possible without the written approval of VULNIT SAS.

VulnIT and its logo are copyrighted.

VULNIT SAS, capital of 94 000 € -

RCS Nanterre - Siret 518 441 647 00014 - VAT FR 84 518 441 647 -

Headquarters: 75, av. Victor Hugo. 92500 Rueil-Malmaison - France