



[VULNIT]

Vulnerability
Identification Tool

VulnIT – Plug & Audit

USER GUIDE

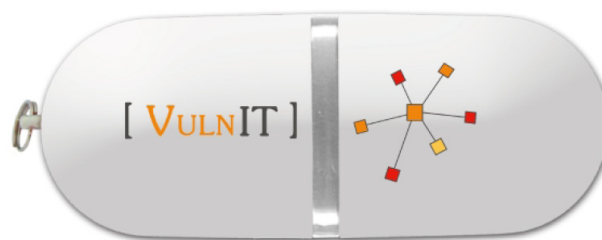


Table of contents

- Table of contents..... 2

- Quick start 4
 - Pre-requisites 4
 - Plug the USB key..... 4
 - Boot 4
 - License activation 5
 - Input the target(s) or use automatic discovery..... 6
 - Validate acquisition 8
 - Test execution 9
 - View the report 9
 - Save the report..... 10
 - Start a new audit 11

- Wifi Audit..... 12
 - Opening the wifi console..... 12

- Windows shares audit 13
 - Opening the Windows shares console 13

- Advanced functionality..... 15
 - Opening a report 15
 - Network interface 15
 - Proxy (Internet connection) 16
 - Change the software language..... 16
 - Change the boot password 17

Changing the test email address.....	17
View and save audit logs	18
Wordlists	18
Check for updates.....	20
Extract a file (report, log file or wifi snapshot).....	21
Boot VulnIT for Windows	21
Decrypt a file	22
Report transmission	22
Backup and restore	23
Backup	23
Restore	23
Troubleshooting	24
My computer does not boot on a USB key	24
My computer still boots on the hard disk	24
The key does not boot, an error occurs	24
The software does not start	24
The key is not recognized	24
The wifi console does not show up	25
The update process did not terminate correctly	25
I forgot my bootup password.....	25
I forget the password used to save a report	25
Error message.....	25
VulnIT.....	26

Quick start

VulnIT Plug & Audit ships the whole environment used to perform your security audits and thus, requires no installation.

Pre-requisites

In order to use VulnIT Plug & Audit, you must be able to boot a computer (either desktop or laptop) on a USB pendrive.

If USB does not come first in your boot order, you may:

- type a specific key during boot time, allowing you to select the boot device in a list (often F8 or F12), or
- configure your boot sequence (in the BIOS settings by typing Del, F1, F2 or F10 depending on your computer) to give USB the highest priority.

Note: USB may be referred to as 'USB-ZIP' or 'USB-FDD'.

If your computer can not boot on a USB pendrive, or if you do not have access to your boot sequence, you can download a dedicated ISO image from our website:

<http://www.vulnit.com/support.php>, burn it on a CD and insert the CD together with the USB pendrive. The computer will boot on the CD then simply press 'Enter' to continue booting on the USB key.

Plug the USB key

Insert the USB key in any USB port of your computer, power on and select the USB key from the boot menu (as described above).

Boot

The computer automatically boots on the page below, asking for your password. This password is required in order to use VulnIT.

[VULNIT]

First boot

Welcome in VulnIT Plug & Audit
Please setup a password. It will be used to protect future use of this software.

Français

English

Password:

Repeat password:

Display clear-text password

By clicking "I agree" below, you indicate your acceptance of the license agreement and you acknowledge you have read all the terms and conditions of this agreement, understand them, and agree to be legally bound by them. If you do not agree with the terms of this agreement, you may not use the product VULNIT, as such term is defined in this agreement.

Accept

© 2009-2011 VULNIT SAS
All rights reserved

Technical support: (+33) 1 55 94 92 71
Version 4.0 (17/05/2011) - Terms and Conditions

Once the password typed and the language chosen, the VulnIT page appears.

License

- ❖ Current license: T1V2U3L4N5I6T700
- ❖ Type of license: eval
- ❖ Expiration date: 20110602
- ❖ Login:

Activate **Update**

Information

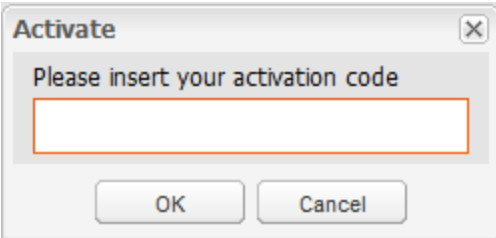
- ❖ Date: 19/05/2011, 12:34:16 (UTC).
- ❖ Version: 4.0.

This page shows general usage information such as the details of your license and the version of the software.

License activation

The evaluation license initialized at first boot is valid for 2 weeks and includes restrictions regarding the amount of details provided in the audit report.

In order to activate your user license for one year, please contact our commercial support who will provide you with a 6-letter activation code. Once the code acquired, click on “Activate” button and then insert it in the prompt window (see figure below).



The license activation is completely automatic, it uses a simple Internet connection , it might however require configuring the software connection with the proxy settings (please refer to the “Proxy” section). The license will be updated automatically.

You cordially invited to contact our commercial support, a month before the end of the license validity period, to command a new one. Otherwise, the software will be locked the day of the license expiration date.

Input the target(s) or use automatic discovery

Scan scope / Specify the target in one of the following forms:

- ✦ DNS name
- ✦ IP address (x.x.x.x)
- ✦ CIDR address (x.x.x.x/yy)
- ✦ Address range (x.x.x.x-y or x.x.x.x-y.y.y.y)
- ✦ Website (http://www.xxx.com)
- ✦ list of any of the above forms separated by “,”
- ✦ or leave it empty to inventory all targets.

Scan depth:

Select port scanning depth:

Fast Normal Complete

Acquire

On the first tab, you may input:

- a target by its domain name (for instance, db.company.lan) or its IP address,
- a range of targets by its CIDR notation (for instance, 192.168.137.0/24) or a dashed notation (from 192.168.137.50 to 192.168.137.128),

- a website by its address (for instance, http://intranet. company.lan), its alias (http://sites. company.lan/alias) or a specific folder (http://sites. company.lan/alias/folder/),
- a list of any of the previous forms separated by commas,

or leave the field empty to automatically discover all the servers in your organization.

You can select the acquisition speed as well by setting the test depth: 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).

Caution: The discovery mode shouldn't be used in the following cases:

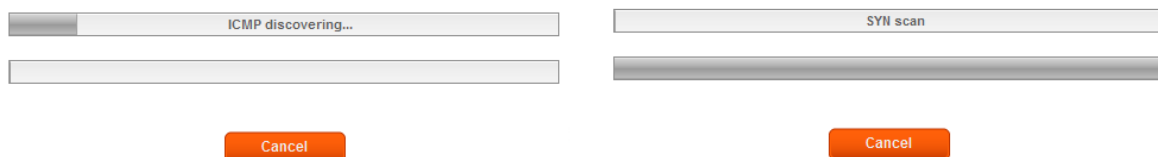
- you do not own all the servers of your internal network (which may also include other subsidiaries servers);
- the network has an IPS (Intrusion Prevention System), port scan would mostly probably block your network;
- the network firewalls implement restriction rules in case of irregular activity.

As a best practice, test VulnIT Plug & Audit first on a development or testing server before targeting a production environment.

Caution: Authentication tests brute force trivial accounts in two trials at most. If your target is setup to lock an account after 3 unsuccessful login attempts, be careful to not perform the same audit twice on the same target.

Note: if you choose the discovery mode and if your computer has several network interfaces, please refer to the « network interfaces » section.

Ports scan phase has 2 steps: target scan (which consists in detecting all reachable devices within the chosen audit perimeter) and service identification (which consists in detecting all open ports on previously detected devices).



You may stop the acquisition process at any time by clicking on the ‘Stop’ button. The progress bar indicates that abort is in progress. Once the acquisition process has been correctly aborted, the audit is reset to let you refine the audit scope.

Validate acquisition

Once this first acquisition phase completed, you'll be automatically forwarded to the “Test” page, in which you can view the identified devices and their services. You have to validate the exact audit scope before executing any test.

Select a target to view its services in the “Services” grid. In order to test a target check it, and to refine your selection furthermore check only specific ports. In checking a target all its services are automatically selected, and the other way around by unchecking a target all its services are unselected.

If you want to test the security of a website on one of the discovered devices, you either have to select its URL in the “Website” grid, or select the port on which operate its web server in the “Services” target.

The screenshot displays a web application interface with several sections:

- Targets:** A table with columns 'Selection', 'IP', 'Name', and 'Netbios name'. It lists 12 IP addresses from 192.168.1.1 to 192.168.1.21. IP 192.168.1.6 is selected. Other names include 'cal.intra-vulnit.com', 'UBUNTU-LAMP', 'ACER', and 'DELL1'.
- Services:** A table with columns 'Selection', 'Port', and 'Name'. It lists three services: SSH (Secure Shell Login) on port 22, HTTP (World Wide Web) on port 80, and PostgreSQL on port 5432. All are selected.
- Website:** A table with columns 'Selection' and 'URL'. It is currently empty.
- Credentials:** A form with four input fields: 'SSH login:', 'SSH password:', 'Windows login:', and 'Windows password:'.

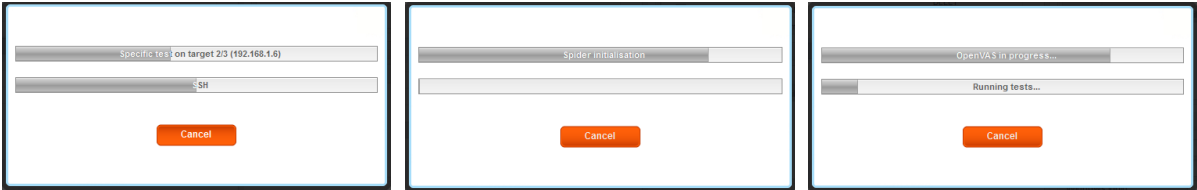
At the bottom of the interface are four orange buttons: 'Scan', 'Save', 'View', and 'Open'.

Regarding patch management testing, you may specify an administrator account (SSH account and/or Windows domain account) to connect to the target and detect the missing patches relative to the local applications installed.

Once the audit perimeter validated, click on the “Scan” button to launch the test.

Test execution

The test execution phase is automatic. The test execution progress is showed in the following windows. The first bar provides the progress of specific tests (regarding a panel of targeted services), the second one provides the progress of web site analysis and crawling, whereas the third one is relative to patch management testing (which relies on OpenVAS).



You may stop the test process at any time by clicking on the ‘Stop’ button. The progress bar indicates that abort is in progress. Once the test process has been correctly aborted, the audit is reset to let you refine the audit scope.

View the report

IP	Title	Function	Object	CVSS	Impact	Exploitability
192.168.1.23	Web patch management	Patch mgt	Web	10.0	10.0	10.0
192.168.1.23	Web patch management	Patch mgt	Web	9.3	10.0	8.6
192.168.1.23	Web patch management	Patch mgt	Web	8.5	10.0	6.8
192.168.1.23	Windows patch management	Patch mgt	Windows	8.5	10.0	6.8
192.168.1.23	Windows patch management	Patch mgt	Windows	7.5	6.4	10.0

Vulnerability: Web patch management
Description: The patches listed below have not been correctly installed. Thus, the relative security vulnerabilities have not been fixed and could be exploited.
Resolution: Install the patches provided by the editor.
CVSS vector: AV:N/AC:L/AU:N/C/I:C/A:C/I
Information about the detection plugin: 900915
Reference: CVE-2009-2853
Fix: WORDPRESS

Once the test phase completed, the newly detected vulnerabilities will be automatically loaded in the “Vulnerabilities” grid. You can view a detailed report of detected vulnerabilities by selecting the targets and by clicking on the “View” button afterward.



A save file dialog will appear to propose opening the report to you.

Note: we do not recommend printing nor saving the report from this view window. A dedicated procedure is described below.

Save the report

In order to save the audit report for future use (print or send it, see the following chapters), please click the 'Save' button.

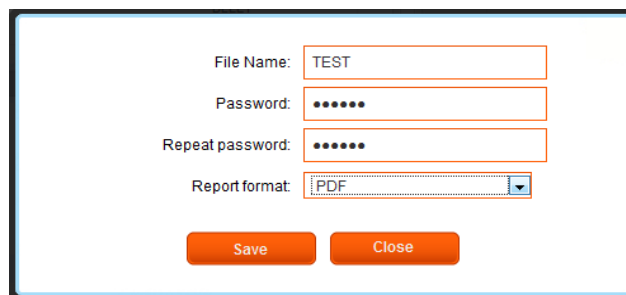


The report name is consisted of two parts a prefix that contain the the time of the generation and a second part chosen by a user. A dialog box prompts you for a name for the report an a password to encrypt it. The password should:

- contains at least eight characters,
- contains at least a number and a letter,
- contains no sequences of numbers or letters.

You may choose a different password for each report (in particular, we recommend you choose another password than the password used at boot time to log in the software).

Caution: if you forget the password used to encrypt a report, no one will be able to decrypt it.

A screenshot of a save dialog box. It contains four input fields: 'File Name' with the text 'TEST', 'Password' with six dots, 'Repeat password' with six dots, and 'Report format' with a dropdown menu showing 'PDF'. At the bottom, there are two orange buttons labeled 'Save' and 'Close'.

Option: if you acquired the extended export option, you can export the report in several formats: PDF (by default) to obtain a non modifiable report, CSV in order to integrate the content of the report in Microsoft Excel for instance, or MHT (equivalent to HTML) if you wish to edit the report, using Microsoft Word for instance.

Choose the format you want to use in the 'File type' list.

The recording of the report is confirmed a dialog box.

Start a new audit

To start a new audit, you can either launch a new target acquisition in the "Scan" page, or launch an analysis scan on already discovered targets in the "Test" page and repeat the steps described in "Audit Validation".

Wifi Audit

Opening the wifi console

If order to audit wifi security, click 'Plugin' and 'Wifi console'. A new window (similar to the window below) shows up.

Select the WiFi interface

BSSID	SSID	Power	Channel	Algorithm	Cypher	Authentication	Risk
00:1B:2F:47:46:26	XXXXXXXXXXXXXX	📶	6	WPA2	CCMP	PSK	Low
C0:C1:C0:18:6A:10	XXXXXXXXXXXXXX	📶	11	WPA2	CCMP TKIP	PSK	Low
00:26:16:2D:F0:20	VULNIT	📶	11	WPA2/WPA	CCMP TKIP	PSK	Low
00:12:17:16:10:86	XXXXXXXXXXXXXX	📶	6	WPA2	CCMP	PSK	Low
00:17:33:47:A9:80	XXXXXXXXXXXXXX	📶	11	WEP	WEP		Medium
00:18:4D:37:AE:24	XXXXXXXXXXXXXX	📶	1	WPA2	CCMP	PSK	Low
F2:6E:07:BC:AC:B1	XXXXXXXXXXXXXX	📶	12	WPA2	CCMP	PSK	Low
F2:6E:07:BC:AC:B2	XXXXXXXXXXXXXX	📶	12	OPN			High
F2:6E:07:BC:AC:B0	XXXXXXXXXXXXXX	📶	12	WPA2	CCMP	PSK	Low
F2:6E:07:BC:AC:B3	XXXXXXXXXXXXXX	📶	12	WPA	TKIP	MGT	None
00:1F:C6:5C:33:48	XXXXXXXXXXXXXX	📶	4	WPA	TKIP	PSK	Low
72:64:EA:31:9E:BD	XXXXXXXXXXXXXX	📶	12	WPA2	CCMP	PSK	Low
72:64:EA:31:9E:BE	XXXXXXXXXXXXXX	📶	12	OPN			High
72:64:EA:31:9E:BF	XXXXXXXXXXXXXX	📶	12	WPA	TKIP	MGT	None
00:1C:F0:F5:37:E6	XXXXXXXXXXXXXX	📶	4	WPA2/WPA	CCMP TKIP	PSK	Low
00:26:F2:DD:B3:BF	XXXXXXXXXXXXXX	📶	6	WEP	WEP		Medium

A list of access points appears.

The 'Algorithm', 'Encryption', 'Authentication' and 'risk level' columns describe the security settings of each access point.

Click on each column name to sort the access points.

If you have several wifi interfaces on your computer, you may choose which interface to use in the list at the top of the window.

You can click 'Export' to take a snapshot of the console. The procedure is similar to saving a report (see above).

Windows shares audit

Opening the Windows shares console

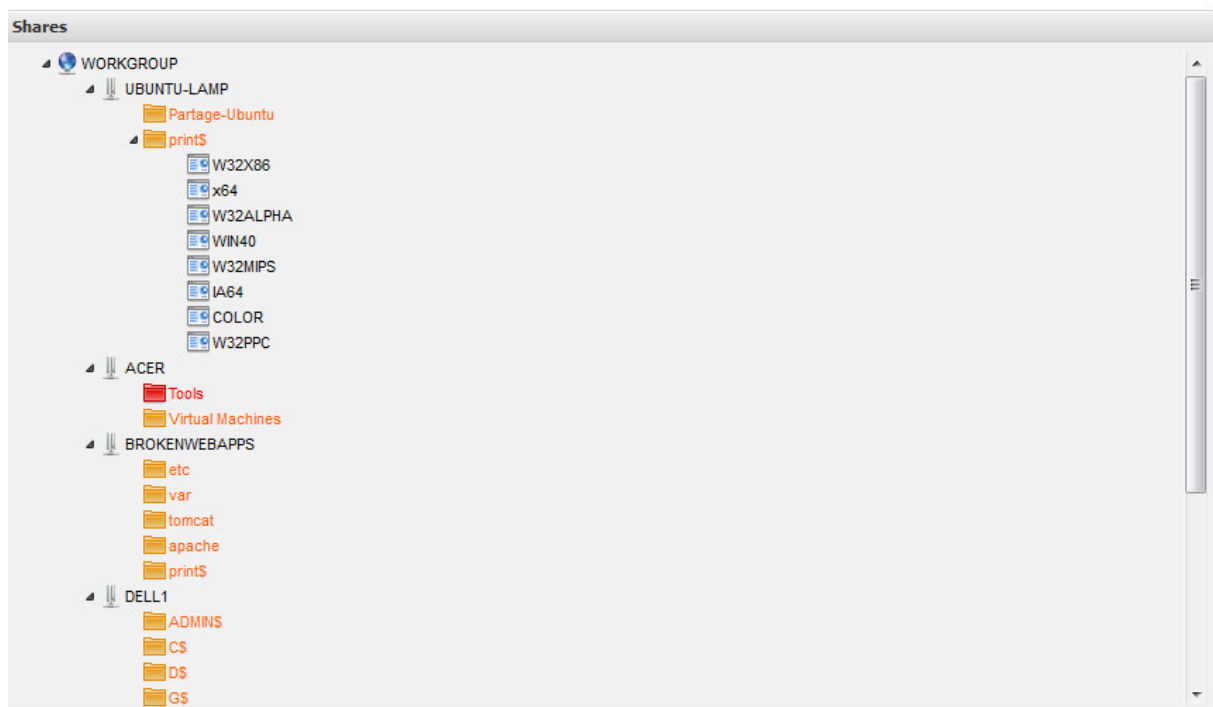
Option: the console can only be accessed if you acquired this option.

If your wish to open the Windows shares console, click 'Plugins' then 'Samba console'. A new window (similar to the window below) shows up.

Domain to crawl:

User:

Password:



This console lists the Windows (Samba) file shares discovered on a domain or workgroup, represented as a tree similar to the 'Network neighborhood' provided by Windows explorer.

This tree contains the list of all the servers accessible in the selected domain, and, for each server, the list of folders shared on this server and if the user has read-only (yellow for [RO]) or read-write (red for [RW]) access to these folders.

First, choose the domain you wish to crawl among the detected domains in the listbox.

You can provide a domain account which will let you see the list of servers and folders accessible to this account. You may also leave these two fields empty in order to detect the file shares open to everyone.

Click 'Start' to start crawling. You can interrupt the process at any time.

At the end of the process, the tree is populated in the bottom part of the window. You can click 'export' to take a snapshot of the console. The procedure is similar to saving a report (see above).

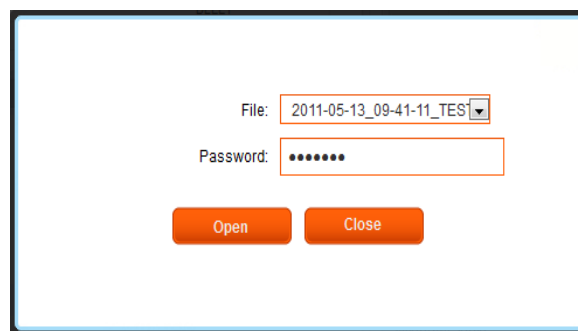
Advanced functionality

Opening a report

In order to view a report previously generated and saved on the USB key, go to the “test” page, and click on the ‘Open’ button. Choose your report in the dialog box.

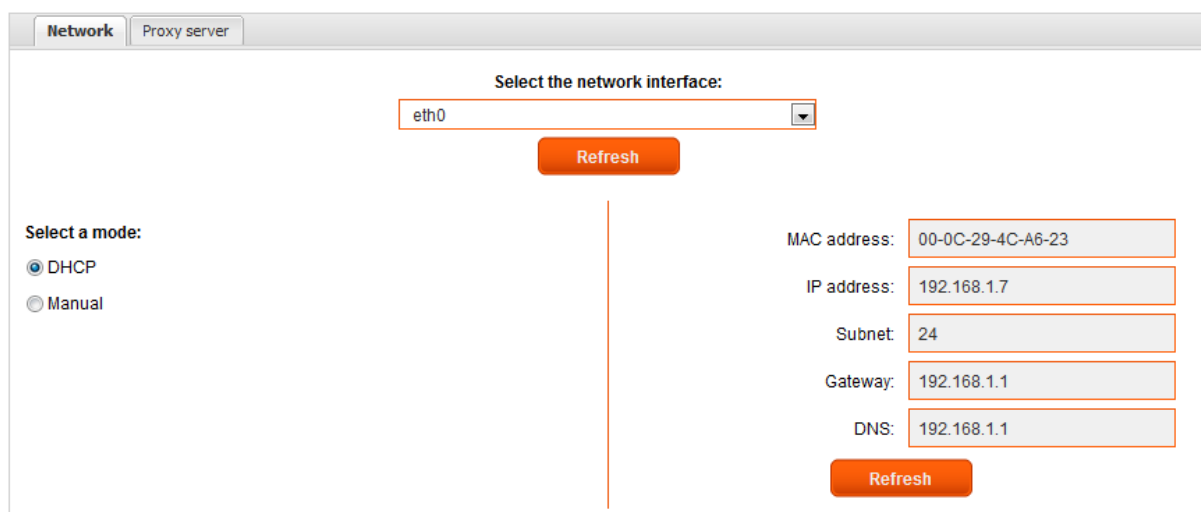


Enter the password used to encrypt the report. The decrypted report will be displayed in a new window.



Network interface

If your computer has several network interfaces (ethernet interfaces only, as VulnIT does not support auditing via a wifi interface), you may choose which interface to use by clicking on the ‘Configuration’ menu and then choose ‘Interface’. Select the interface you want to use and click ‘Select’.



Each interface may be setup in DHCP (automatic IP addressing). You may want to renew the IP address if you plugged your network cable after the software has booted for instance.

You may also configure your network interface manually, by specifying the IP address, the subnet mask, the gateway and a DNS server. Then click 'Save'.

Proxy (Internet connection)

If you use a proxy to connect to the Internet, you may need to configure this connection in order to get the latest updates from our website.

To do so, click on the menu 'Configuration' and then 'Proxy' and fill in the proxy server address and port (for instance, 8080). If your proxy requires an authentication, add your username and password. The password will not be saved (for security considerations), so you will be asked to input your password at each boot.

If the proxy authentication relies on the Windows domain authentication, input the domain name in order to register your computer in the domain and enable the Internet connection.

The screenshot shows a configuration window with two tabs: 'Network' and 'Proxy server'. The 'Proxy server' tab is selected. The window is divided into two main sections. The left section, titled 'Proxy server', contains two input fields: 'Address:' and 'Port:'. The right section, titled 'Authentication (standard, NTLM, Kerberos)', contains three input fields: 'Realm (kerberos domain):', 'User:', and 'Password:'. A 'Save' button is positioned at the bottom center of the window.

If the proxy authentication relies on the Windows domain authentication, input the domain name in order to register your computer in the domain and enable the Internet connection.

Note: If this connection fails, you may configure your proxy to allow connections to 'update.vulnit.com' which is the domain used to get VulnIT updates.

Change the software language

In order to change the language of the software (both interface and report), click on the 'Configuration' menu and then choose 'Language'. Select your language in the list and click OK.

Language / Choose the user interface language

Français

English

Save

Keyboard / Choose the keyboard layout

Layout:

Save

If this code is not recognized, the USA keyboard layout will be used by default.

Change the boot password

The password required for booting VulnIT (at startup) can be modified using the 'Configuration' menu and item 'Password'.

You have to input the old password, then twice the new one, and click "Change".

Password / Change password

Old password:

New password:

Repeat new password:

Change

Changing the test email address

Testing a mail server requires sending an email in order to accurately detect its potential vulnerabilities (see example below). To change it go to the "configuration" menu and choose "email address" item. Insert your new email and then click on the "change" button to save changes.

Set an email address to get more accurate SMTP testing

Email address:

Change

View and save audit logs

The audit logs generated by VulnIT can be viewed using the log console (click on the the “log” link the header). You can specify the type of log you want to view by using the checkboxes at the top of the window.

Each line begins with the time (hour, minute, second and millisecond) this line was generated.

These logs are flushed at each reboot. If you wish to keep these logs, click ‘Save’ at the top of the log console. The save procedure is similar to saving a report (see above).

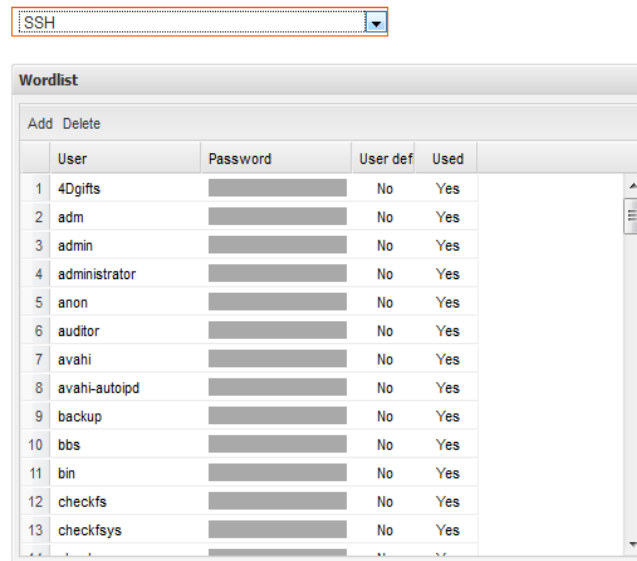
Horodatage	Message
2011-05-17 09:47:00.543	Initializing target acquisition
2011-05-17 09:47:00.566	Creating targets
2011-05-17 09:47:00.646	Get all available targets
2011-05-17 09:47:00.65	C[8]: ip -o -f inet addr show dev eth0 scope global awk '{print \$4}'
2011-05-17 09:47:00.775	A[8]: 192.168.1.7/24
2011-05-17 09:47:00.884	C[9]: /media/TOOL/tools/fping/fping -r1 -i10 -t200 -a -g 192.168.1.7/24 2>/dev/null
2011-05-17 09:47:11.096	A[9]: 192.168.1.7
2011-05-17 09:47:11.113	A[9]: 192.168.1.9
2011-05-17 09:47:11.115	A[9]: 192.168.1.14
2011-05-17 09:47:11.116	A[9]: 192.168.1.16
2011-05-17 09:47:11.117	A[9]: 192.168.1.21
2011-05-17 09:47:11.118	A[9]: 192.168.1.13
2011-05-17 09:47:11.12	A[9]: 192.168.1.19
2011-05-17 09:47:11.204	C[10]: dig @192.168.1.1 +short +tries=1 +time=2 -x 192.168.1.9 grep -v "timed out"
2011-05-17 09:47:11.316	A[10]:
2011-05-17 09:47:11.421	Reading Netbios information
2011-05-17 09:47:11.423	C[11]: nmblookup -s /dev/null -A 192.168.1.9 grep '<20>' awk '{print \$1}'
2011-05-17 09:47:11.535	A[11]: UBUNTU-LAMP
2011-05-17 09:47:11.637	C[12]: nmblookup -s /dev/null -A 192.168.1.9 grep '<1e>' head -n 1 awk '{print \$1}'
2011-05-17 09:47:11.761	A[12]: WORKGROUP
2011-05-17 09:47:11.869	C[13]: dig @192.168.1.1 +short +tries=1 +time=2 -x 192.168.1.14 grep -v "timed out"
2011-05-17 09:47:11.998	A[13]:
2011-05-17 09:47:12.099	C[14]: nmblookup -s /dev/null -A 192.168.1.14 grep '<20>' awk '{print \$1}'
2011-05-17 09:47:12.22	A[14]: DELL1
2011-05-17 09:47:12.322	C[15]: nmblookup -s /dev/null -A 192.168.1.14 grep '<1e>' head -n 1 awk '{print \$1}'

Wordlists

VulnIT integrates predefined wordlists of common user accounts, database instances, SNMP communities, etc.

You can enhance these lists by adding a new word or user account, corresponding to the name of the application tested, the name of your company, or the name of your system administrator for instance.

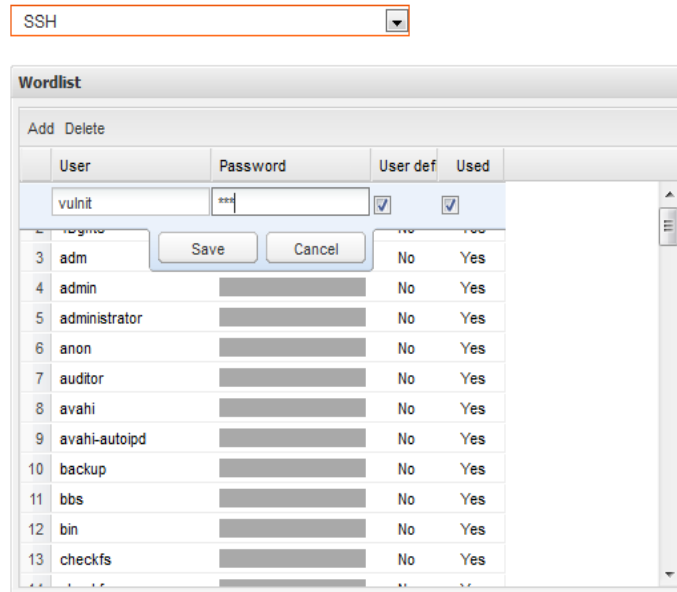
Follow the 'Configuration' menu, then 'Wordlists'. The following window shows up:



First, choose the dictionary you want to modify in the listbox. Depending of your choice, you will be able to insert a new word (for instance, an SNMP community name or an SSH account, as showed above).

The user accounts which passwords cannot be parametered (SSH accounts for instance) are tested with a trivial password, i.e. a password identical to the login or an empty (null) password.

The list of predefined words appears. If you wish to remove a word, select it and then press on the delete button at the top on the grid. In order to add a new word, press on the "add" button. Input the word of your choice, check the corresponding box and press "save".



Check for updates

If you can connect to the Internet (if you cannot, please refer to the Proxy chapter above), the software will automatically check for updates and suggest to download them.

If you accept, the updates will be downloaded. The software will close during installation and restart automatically at the end of the installation.

You may also request for updates manually by going to the “Home” page and click on “Update”.

License

- ❖ Current license: T1V2U3L4N5I6T700
- ❖ Type of license: eval
- ❖ Expiration date: 20110602
- ❖ Login:

Activate
Update

Information

- ❖ Date: 19/05/2011, 12:34:16 (UTC).
- ❖ Version: 4.0.

Extract a file (report, log file or wifi snapshot)

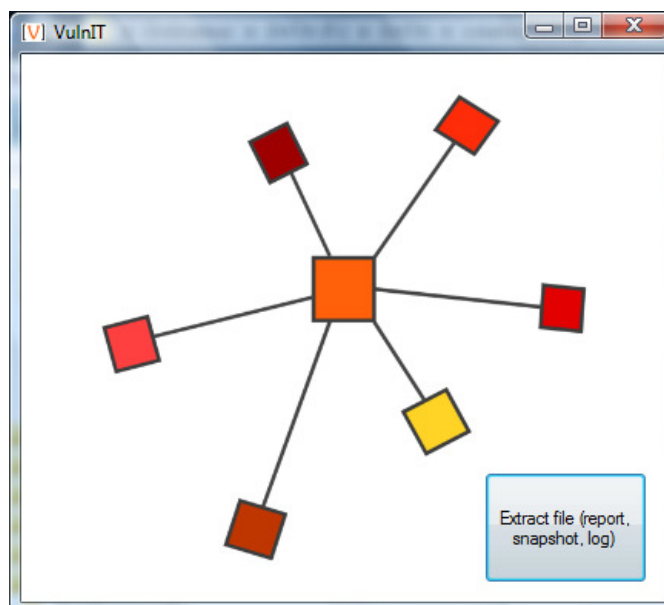
Boot VulnIT for Windows

The VulnIT Plug & Audit key may be inserted in a Windows environment in order to view the reports, audit logs and wifi snapshots saved previously. The common use of this software consists in extracting a report and printing it. If you wish to transfer a file by email or CD, you should refer to the 'Transmission' chapter below.

When you insert the key in a Windows environment, the automatic startup menu lets you execute VulnIT.

Note: This automatic startup menu may be deactivated on your computer. If no popup menu appears when plugging the USB key, explore the key manually and start the 'VulnIT.exe' program.

A new window shows up (if you have installed .Net Framework 1.1 or above, otherwise the same functionalities will be provided in another form).



Decrypt a file

Click 'Extract a file'.

Select the file you want to decrypt (by browsing the logs, reports and snapshots directories), then the folder in which you want to save the file.

Caution: the extracted file must not be saved on the key, in order to only keep encrypted files on the pendrive.

Finally, input the password that was initially used to save the file.

The file will be extracted in the selected folder. The encrypted file remains on the USB key.

Report transmission

If you wish to send the audit report (by email for instance), we recommend you send the report in its encrypted form (.bfe format), by exploring the 'reports' folder of the USB key, and the related password by another mean (by phone for instance).

The recipient can decrypt the report with its own VulnIT Plug & Audit key by copying the file in the 'reports' folder of its key.

The recipient may also use a dedicated online tool:

<http://www.vulnit.com/decrypt.php>

Note: The audit reports decrypted using the above webpage are deleted immediately after being downloaded and thus, neither accessible nor stored.

Backup and restore

Backup

In order to prevent any data loss (reports, audit logs and wifi snapshots) in case of USB key failure, you may backup these files regularly by simply copying the 'reports', 'logs' and 'snapshots' folders of the USB key to another media.

Restore

Should the case arise, you may restore your reports, audit logs and wifi snapshots by replacing the 'reports', 'logs' and 'snapshots' folders of your USB key.

Troubleshooting

My computer does not boot on a USB key

The older computers do not support booting on a USB key. If this is the case, either try to find a newer computer to boot on, or get from our website (on the 'Support' page) a CD ISO image dedicated to this problem.

Burn this image, insert the CD and boot your computer. The CD will start and switch to the USB key.

My computer still boots on the hard disk

Check the boot sequence in your BIOS settings. If you do not know how to configure this sequence, or if you are not allowed to change it, contact your administrator.

The key does not boot, an error occurs

When booting, if the computer reports that the USB key is not a bootable device, the key may have a material deficiency.

Please contact our technical support. We will proceed to a replacement by a reconditioned part. If you had already produced and saved audit reports and if they are still reachable, they will be transferred to the new key. If you have backed-up your key, you will be able to replace the files on the new key.

The software does not start

The computer boots, but no window appears and nothing happens. This may occur when an update hangs or mistakenly stops. In this case, please contact our technical support.

The key is not recognized

At boot time, the software indicated that the USB key is not recognized. In this case, we will proceed to a replacement by a reconditioned part.

The wifi console does not show up

The wifi console requires a compatible wifi interface. If your computer does not have a wifi interface, or if the wifi interface is not recognized by the operating system, we can provide you with a list of compatible devices.

The update process did not terminate correctly

The software closed during update installation but it did not started again. If you waited for at least 15 minutes and if your computer shows no activity, press ctrl - alt - del to reboot your computer properly.

Is the problem persists, or if the software no longer starts at boot time, please contact our technical support.

I forgot my bootup password

If you forgot the password required at boot time, it is impossible to retrieve it. You must return the key and we will proceed to a replacement by a reconditioned part.

I forget the password used to save a report

If you forgot a password used to save a report, there is no way to retrieve it, or replace it. This report is useless.

Error message

If you do not understand an error message, do not hesitate to contact us.

VulnIT

Technical documentation:

www.vulnit.com/support.php

www.vulnit.com/ressources.php

Contact:

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 75 000 € -
RCS Nanterre - Siret 518 441 647 00014 - VAT FR 84 518 441 647 -
Headquarters: 75, av. Victor Hugo. 92500 Rueil-Malmaison - France