



[VULNIT]
Vulnerability
Identification Tool

VulnIT-VM

USER GUIDE

Table of contents

First boot	4
Pre-requisites	4
Configuring and Deploying the VM	4
Access the VM	4
Vulnerability discovery and monitoring	6
Network topology discovery	6
Tests scheduling	7
Assets inventory	8
Vulnerabilities details	9
Using tickets	10
Dashboard	11
Report generation	12
Windows shares audit	14
Opening the Windows shares console	14
Groups and users management	16
Change the boot password	16
Create an assets group	16
Manage users	16
Advanced configuration	18
Network interface	18
Proxy (Internet connection)	18
Customize wordlists	19
Change the software language.....	20
Change the test email address.....	20
Change the default credentials	20

Other Functionalities..... 22

 View and save audit logs 22

 License information..... 22

 Check for updates..... 23

VulnIT..... 24

First boot

Pre-requisites

In order to use VulnIT-VM, you must have a virtualisation infrastructure and client machine with a recent web browser (IE7 and above, Firefox, or Chrome).

Configuring and Deploying the VM

Using the VulnIT-VM solution requires deploying and starting the virtual machine, then use a web browser in order to gain access to it.

The deployment of the virtual machine is described in the online guide:

http://www.vulnit.com/en/doc/VulnIT_deployment_guide.pdf

Once the VM installed in your virtualisation infrastructure, you can start it and configure its network access following the quick start guide:

http://www.vulnit.com/en/doc/VulnIT_VM_quick_start.pdf

Access the VM

Once the virtual machine is installed and started, you can have access to VulnIT-VM web interface by visiting its main page using its IP address, for example:

<http://192.168.1.26>.

In the first boot, you will be prompted to choose the interface language, create a user, and agree with the software license.

First boot

Welcome to Vulnit-VM
Please fill this form online in order to activate your trial version: [link](#).
Then, insert the **same** information here with the generated code.

Name:

First Name:

Company:

Email address:

Code:

Please insert a login and a password. This credentials will be used to encrypt the program results and data

Français

English

Login:

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-VM, as such term is defined in this agreement.

Accept

Once the user is created and the primary language chosen, you will be redirected to the main page of the VulnIT-VM.

Vulnerability discovery and monitoring

Network topology discovery

You can discover your network topology by clicking on the 'Scan' tab in the horizontal panel at the top of the main page.

The screenshot shows the 'Scan scope / Specify the target in one of the following forms:' section with a list of target types: 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 ",", and or leave it empty to inventory all targets. Below this is a text input field for 'Scan scope:' containing '192.168.1.10-20, 192.168.1.33'. The 'Select port scanning depth:' section has three radio buttons: 'Fast', 'Normal' (selected), and 'Complete'. An orange 'Acquire' button is located below the form.

You can configure your scan in multiple ways either by:

- 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.

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

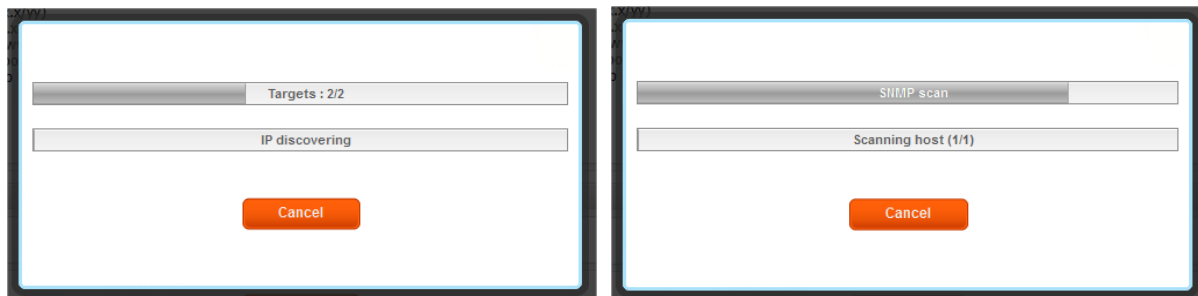
- you do not own all the servers of your internal network (which may also include other subsidiaries servers);
- the network has an IPS (Intrusion Prevention System), port scan would mostly probably block your network;
- the network firewalls implement restriction rules in case of irregular activity.

As a best practice, run VulnIT-VM scanner 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.

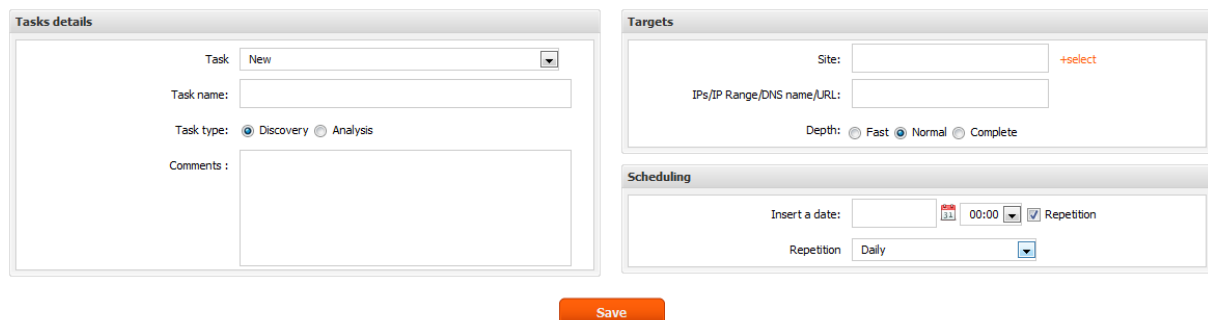
Ports scan phase has 2 steps: target scan (which consists in detecting all reachable devices within the chosen audit perimeter) and service identification (which consists in detecting all open ports on previously detected devices).



You may stop the discovery process at any time by clicking on the ‘Stop’ button. The progress bar indicates that abort is in progress.

Tests scheduling

Once your network is scanned and discovered, you can schedule tasks (discovery, analysis) by clicking on the ‘Tasks’ tab at the top banner.

The image shows a screenshot of a web interface for scheduling tasks. It is divided into three main sections: 'Tasks details', 'Targets', and 'Scheduling'. 'Tasks details' has a dropdown for 'Task' (set to 'New'), a text field for 'Task name', radio buttons for 'Task type' (Discovery selected, Analysis unselected), and a text area for 'Comments'. 'Targets' has a 'Site' dropdown (with '+select' next to it), a text field for 'IPs/IP Range/DNS name/URL', and radio buttons for 'Depth' (Fast, Normal selected, Complete). 'Scheduling' has a date picker, a time dropdown (set to '00:00'), a checked 'Repetition' checkbox, and a dropdown for 'Repetition' (set to 'Daily'). An orange 'Save' button is centered below the forms.

You can give a name to a task in order to easily identify it as well as its type (discovery or analysis). A ‘Discovery’ task allows discovering new machines and services on the network, whereas an ‘Analysis’ task allows you to create automatic security assessments of your IT assets.

For a discovery task, you can precise:

- what IP range to scan (as described in the previous section)
- the date and a time at which the task is launched and at which frequency

For an analysis task, you can precise:

- which targets, services, and website to analyze

- the date and a time at which the task is launched and at which frequency

Once a task is created, it will appear in the drop down list of your created tasks, you can deactivate a tasks at anytime and activate it once again.

Assets inventory

You can consult the list of machine composing your network by clicking on the 'Assets inventory' tab. You can view their details, ports, websites and vulnerabilities.

The screenshot displays the 'Assets inventory' interface. On the left, a 'Sites' panel shows a tree view under 'Main' with 30 IP addresses from 192.168.1.1 to 192.168.1.30. On the right, a 'Targets' panel shows a table of selected targets with their risk levels and open tickets.

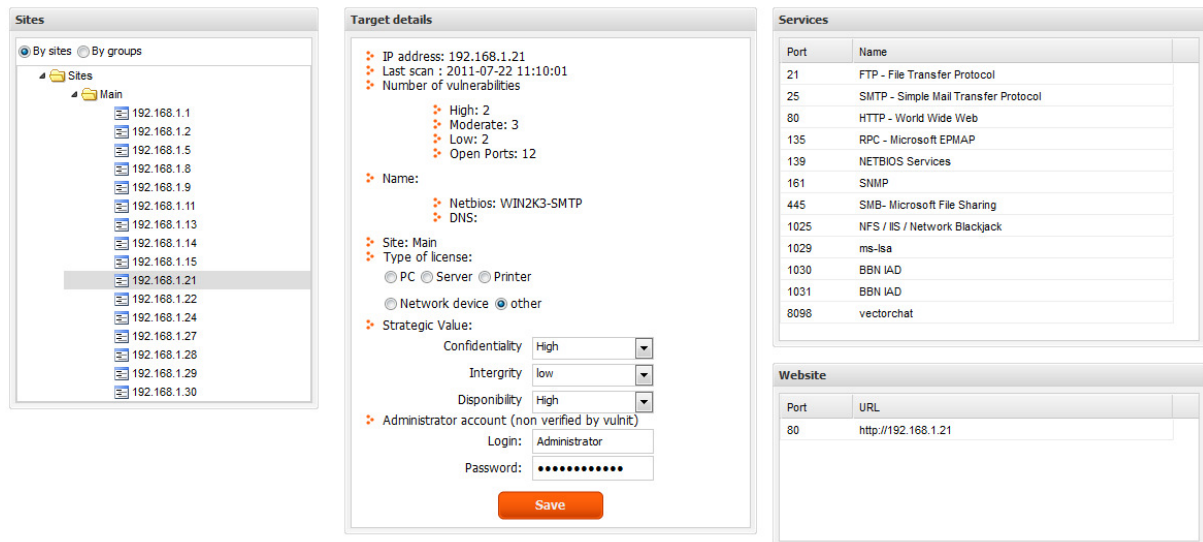
Selection	Name	IP	High	Moderate	low
<input type="checkbox"/>	unknown	192.168.1.1	0	0	1
<input checked="" type="checkbox"/>	cal.intra-vulnit.com	192.168.1.2	1	1	10
<input type="checkbox"/>	unknown	192.168.1.5	0	0	0
<input type="checkbox"/>	unknown	192.168.1.8	0	0	0
<input type="checkbox"/>	W2K8-DC	192.168.1.9	1	0	0
<input checked="" type="checkbox"/>	W2K8-MOSS2007	192.168.1.11	0	0	0
<input type="checkbox"/>	DELL1	192.168.1.13	0	0	0
<input type="checkbox"/>	unknown	192.168.1.14	0	0	0
<input type="checkbox"/>	unknown	192.168.1.15	0	0	0
<input checked="" type="checkbox"/>	WIN2K3-SMTP	192.168.1.21	2	3	2

Below the table is a 'Report generation' section with instructions and three buttons: 'Save', 'View', and 'Open'.

You can view a tree of your network at the left of the screen. Your topology view can be organized either by geographical sites or logical groups. Sites and groups nodes are parents whereas the networks assets are leaves.

By selecting or clicking on a parent node you view its children (in this case the composing machines). A grid composed of the site's or group's machines will appear on the right of the screen, it contains general information about each target: the number of vulnerabilities classified in different risk categories (high, moderate, and low) as well as the number of open tickets treating the target's vulnerabilities.

By selection or clicking on a leaf node (a target), its details will appear on the right side of the screen as well as its open ports and existing websites, moreover its discovered vulnerabilities will appear at the bottom of the screen too.



The details information of each target are composed of two parties, a part filled and inquired by VulnIT-VM, it includes its: IP address, last scan date, number of vulnerabilities classified in terms of risk levels, DNS and NetBios name; the second is optional and it is filled and declared by the user, it includes: type (server, client, network device, etc...), its strategic value in terms of confidentiality, integrity and availability, and finally its SSH or Windows credentials.

The declared credentials of each target are verified by later by VulnIT-VM analyzer.

Vulnerabilities details

As described in the previous section by clicking on a target machine on the network tree at the left of the screen, a list of its vulnerabilities will appear at the bottom of the page, this list contains the details of each discovered vulnerability on the machine order by their risk level. You can view a vulnerability details by expanding its row.

Each discovered vulnerability has a discovery 'Occurrence' i.e. the number of times it has been discovered on the same machine before mediating it, as well as a 'Verified' status that indicates if VulnIT-VM has validated its correction in case it has been reported 'resolved'.

In case VulnIT-VM has reported a false positive, and that you want to mask it, please select it and click on the 'Report false positive' button at the top of the grid. Once a vulnerability is flagged as a false positive, it will not appear again in the grid or future generated reports.

In case VulnIT-VM has discovered a vulnerability that you accept or you wish to ignore for another reason, you can select it click on the 'Ignore' button at the top of the grid and it will be highlighted in gray to flag it as accepted.

Vulnerabilities											
<input type="button" value="Select all"/> <input type="button" value="Deselect all"/> <input type="button" value="Marked as false positive"/> <input type="button" value="Add to ticket"/> <input type="button" value="Ignore"/>											
	Selection	#	Title	Function	Object	CVSS	Impact	Exploitab	Close Date	Occrance	Verified
<input type="checkbox"/>	<input type="checkbox"/>	23	Windows patch management	Patch mgt	Windows	10.0	10.0	10.0		1	non verified
<input type="checkbox"/>	<input checked="" type="checkbox"/>	25	Windows access control	Access cont	Windows	9.0	10.0	8.0		1	non verified
<input type="checkbox"/>	<input type="checkbox"/>	18	SNMP community (read)	Configuration	Network	8.5	7.8	10.0		1	non verified
<input type="checkbox"/>	<input type="checkbox"/>	16	Anonymous FTP access	Access cont	Network	8.5	7.8	10.0		1	non verified
<input type="checkbox"/>	<input type="checkbox"/>	15	FTP service	Encryption	Network	7.8	7.8	8.6		1	non verified
<input type="checkbox"/>	<input type="checkbox"/>	17	Open mail relay	Access cont	Network	7.8	6.9	10.0		1	non verified

Using tickets

In order to formalize and keep track of the corrections and actions made for the security of your network, we suggest creating tickets and assigning them to the system's users based on their responsibilities.

To create a ticket, please select one the vulnerabilities or more and then click on the 'Add to a ticket' button at the top of the page. The pop-up screen below will appear:

Ticket:

Summary:

Reported by: Assigned to:

Priority: Due date:

Description:

You can add the selected vulnerabilities either to a new ticket or existing one. In case, you wish to create a new ticket please fill all the needed information and then click on 'Add'.

Ticket:

Summary:

Reported by: Assigned to:

Priority: Due date:

Description:

You can view each vulnerability details by clicking on the ‘Ticket’ tab in the panel at the top of the page.

Ticket: 30 - Apply patches to SQL2K8 servers

Details

Summary: Apply patches to SQL2K8 servers

Reported by: vulnit Assigned to: vulnit

Priority: Very High Due date: 2011-09-23

Description: Specially the SP1!

Vulnerabilities

Select all Deselect all Declared as solved

Selection	#	Title	Function	Object	CVSS	Impact	Exploitability	Close Date	Occranc	Verified
<input checked="" type="checkbox"/>	16	Anonymous FTP access	Access cont	Network	8.5	7.8	10.0		1	non ver
<input checked="" type="checkbox"/>	18	SNMP community (read)	Configuration	Network	8.5	7.8	10.0		1	non ver
<input type="checkbox"/>	15	FTP service	Encryption	Network	7.8	7.8	8.6		1	non ver
<input type="checkbox"/>	17	Open mail relay	Access cont	Network	7.8	6.9	10.0		1	non ver
<input type="checkbox"/>	23	Windows patch management	Patch mgt	Windows	10.0	10.0	10.0		1	non ver
<input type="checkbox"/>	25	Windows access control	Access cont	Windows	9.0	10.0	8.0		1	non ver

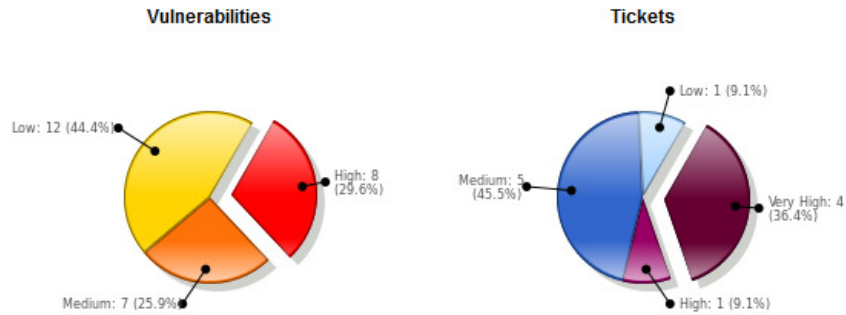
By selecting a ticket from the drop down list, you can view its details such the creator of the ticket, its owner, due date, as well as a description of the required actions. Moreover, you can report a vulnerability corrected upon its correction.

The definite closing state and closure date are filled by the VulnIT-VM analyzer after validating the correction of all vulnerabilities composing the ticket.

Dashboard

You can view multiple dashboards summarizing the state of your network on the main page (‘Home’ tab). You can view information by sites, groups, or all your network assets at once.

The first dashboard shows the number of vulnerabilities classified by their risk level and the number of opened ticket classified by priority.



The second dashboard shows the list of the machines in your network associated with the number of vulnerabilities classified by risk levels and their open tickets.

Name	IP	High	Moderate	low	# Tickets
unknown	192.168.1.1	0	0	1	2
cal.intra-vulnit.com	192.168.1.2	1	1	10	6
unknown	192.168.1.5	0	0	0	0
unknown	192.168.1.8	0	0	0	0
W2K8-DC	192.168.1.9	1	0	0	0
W2K8-MOSS2007	192.168.1.11	0	0	0	0
DELL1	192.168.1.13	0	0	0	0
unknown	192.168.1.14	0	0	0	0
unknown	192.168.1.15	0	0	0	0
WIN2K3-SMTP	192.168.1.21	2	3	2	1
WIN2K5	192.168.1.22	1	0	1	2

Finally, the third dashboard at the bottom of the page shows the list of vulnerabilities discovered on the network, ordered by their CVSS note (risk level out of 10) associated with their details. You can view opened tickets associated on the network too by selecting this view option at the top of the grid.

Report generation

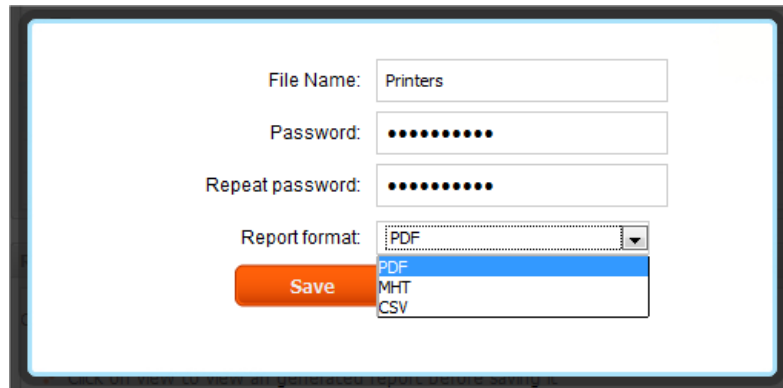
You can generate custom made reports by clicking on the 'Asset Inventory' tab, and choosing the targets you wish to include in the report. A popup window will appear by clicking on the "save" button, it prompts the user for a name, a file format and an encryption password. The designated name will be added to the date and hour of generation.

The password should:

- contain at least eight characters,
- contain at least a number and a letter,
- contain no sequence 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.



The image shows a dialog box for saving a report. It has four input fields: 'File Name' with the text 'Printers', 'Password' with ten black dots, 'Repeat password' with ten black dots, and 'Report format' with a dropdown menu showing 'PDF', 'MHT', and 'CSV'. Below these fields is an orange 'Save' button.

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.

Windows shares audit

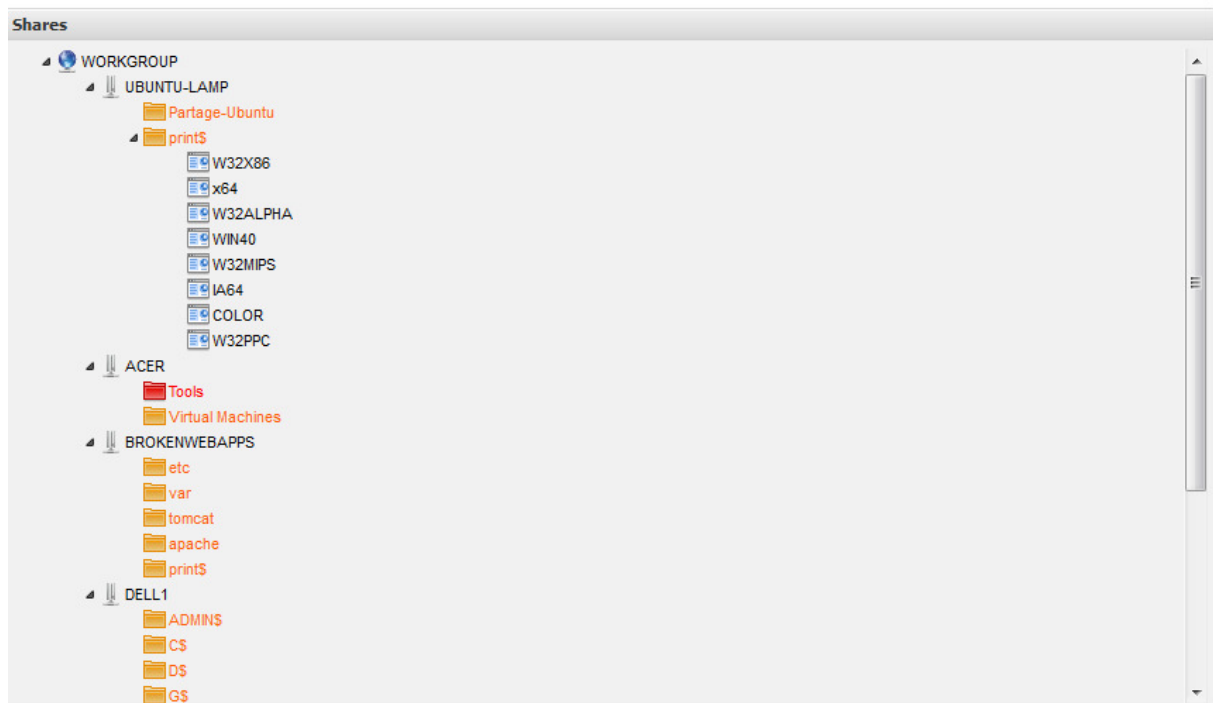
Opening the Windows shares console

If you 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.

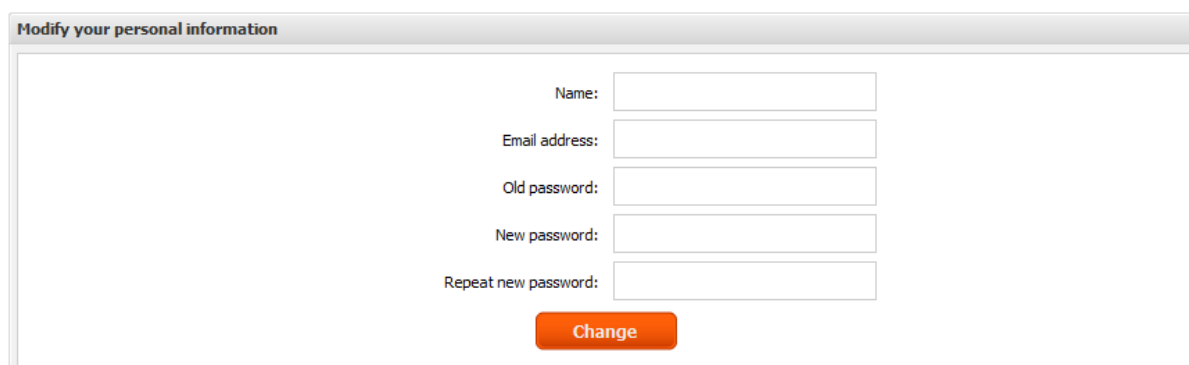
At the end of the process, the tree is populated in the bottom part of the window. You can click 'Export' to take a snapshot of the console. The procedure is similar to saving a report (see above).

Groups and users management

Change the boot password

The password required for booting VulnIT-VM (at login) 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'.

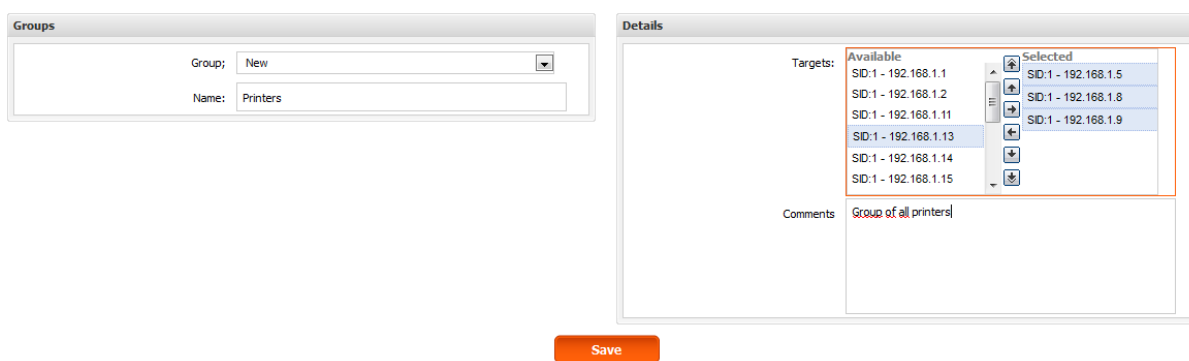


The screenshot shows a web form titled "Modify your personal information". It contains five input fields: "Name:", "Email address:", "Old password:", "New password:", and "Repeat new password:". Below the fields is an orange "Change" button.

Create an assets group

In order to facilitate report editing and tasks scheduling and planning, VulnIT-VM offers the option of the creation of logical groups (for instance, a user can create a group of FTP servers, or printers, or web servers, etc).

To create a group click of the administration tab at the top panel and choose target groups from the menu, the following screen will appear.



The screenshot shows two panels. The "Groups" panel on the left has a "Group:" dropdown menu set to "New" and a "Name:" text input field containing "Printers". The "Details" panel on the right shows a "Targets:" list with two columns: "Available" and "Selected". The "Available" list contains IP addresses from 192.168.1.1 to 192.168.1.15. The "Selected" list contains IP addresses 192.168.1.5, 192.168.1.8, and 192.168.1.9. Below the targets is a "Comments:" text area containing "Group of all printers". An orange "Save" button is located at the bottom center.

This page offers you the possibility of creating a new group as well as deleting an existing one or simply modifying it. In case, you wish to create a new group start by choosing a name for the group and then add the target/machines you want to add to the newly created group. You can add a comment to the group in order to give it a clear definition. Once all the information filled, you click on save.

Manage users

You can either add new administrators to the system to balance the administration load or create users with a restricted access limited to the tickets in order to update the state of the currently opened tickets.

General Information

User:

Login:

Name:

Email address:

Authorisatio

Unrestricted access

Access tickets only

Change your password

New password:

Repeat new password:

An administrator access allows its owner to access all the information offered by VulnIT-VM, whereas a limited access restrict its owner for almost all the functionalities beside updating and accepting open tickets.

Advanced configuration

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'.

The screenshot shows the 'Network' configuration page. At the top, there are two tabs: 'Network' and 'Proxy server'. Below the tabs, there is a section titled 'Select the network interface:' with a dropdown menu showing 'eth0'. Below the dropdown is an orange 'Select' button. To the left of the main configuration area, there is a section titled 'Select a mode:' with two radio buttons: 'DHCP' (selected) and 'Manual'. To the right, there are several input fields: 'MAC address' (00-0C-29-4C-A6-23), 'IP address' (192.168.1.26), 'Subnet' (24), 'Gateway' (192.168.1.1), and 'DNS' (192.168.1.1). At the bottom right, there is an orange 'Refresh' button.

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.

Proxy server configuration window showing fields for Address, Port, Realm (kerberos domain), User, and Password, with a Save button.

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.

Customize 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'.

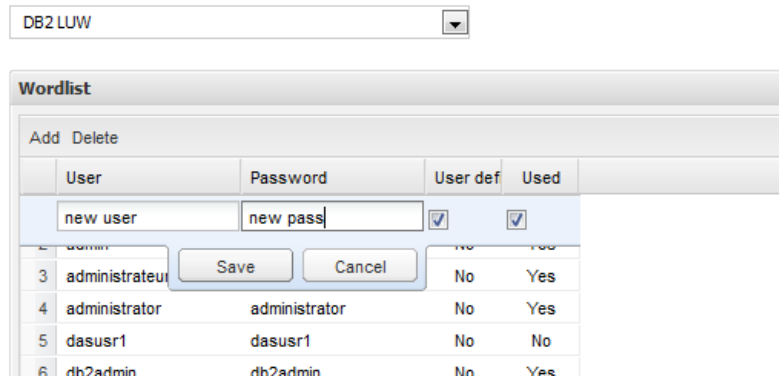
Wordlist configuration window showing a table of user accounts and passwords, with a Save button.

	User	Password	User def	Used
1	admin	admin	No	Yes
2	administrateur	administrateur	No	Yes
3	administrator	administrator	No	Yes
4	dasusr1	dasusr1	No	No
5	db2admin	db2admin	No	Yes
	db2as	db2as	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8	db2fenc1		No	Yes
9	db2fenc1	ibmdb2	No	Yes
10	db2inst1	db2inst1	No	Yes

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'.

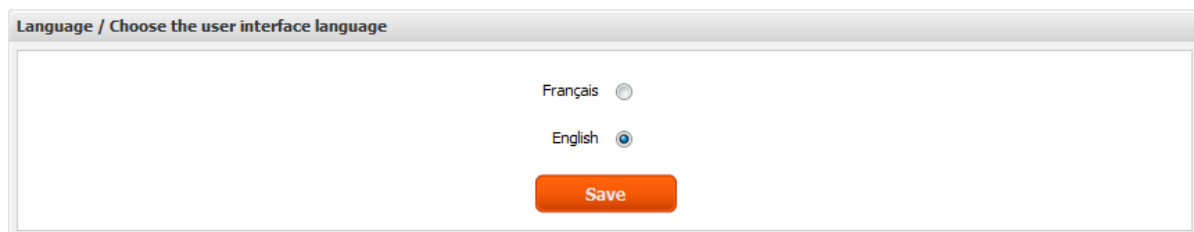


The screenshot shows a 'Wordlist' window with a dropdown menu at the top set to 'DB2 LUW'. Below the dropdown are 'Add' and 'Delete' buttons. A table lists users with columns for 'User', 'Password', 'User def', and 'Used'. The first row is highlighted in blue and contains 'new user', 'new pass', and checked boxes for 'User def' and 'Used'. Below the table are 'Save' and 'Cancel' buttons.

	User	Password	User def	Used
1	new user	new pass	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	admin		No	Yes
3	administrateur		No	Yes
4	administrator	administrator	No	Yes
5	dasusr1	dasusr1	No	No
6	db2admin	db2admin	No	Yes

Change the software language

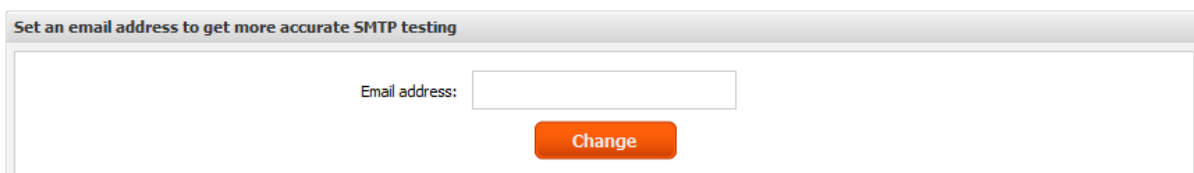
In order to change the language of the software (both interface and report), click on the 'Configuration' menu and then choose 'Language'. Select your language in the list and click OK.



The screenshot shows a 'Language / Choose the user interface language' window. It contains two radio buttons: 'Français' (unselected) and 'English' (selected). Below the radio buttons is an orange 'Save' button.

Change 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 the 'Email address' item. Insert your new email and then click on the 'Change' button to save changes.



The screenshot shows a 'Set an email address to get more accurate SMTP testing' window. It features an 'Email address:' label followed by an empty text input field. Below the input field is an orange 'Change' button.

Change the default credentials

The user can specify common SSH/Windows remote access credentials to the network.

These credentials will be used by the VulnIT-VM analyzer to perform white box tests on the targets.

Default authentication parameters

SSH login :

SSH password :

Windows login :

Windows password :

Change

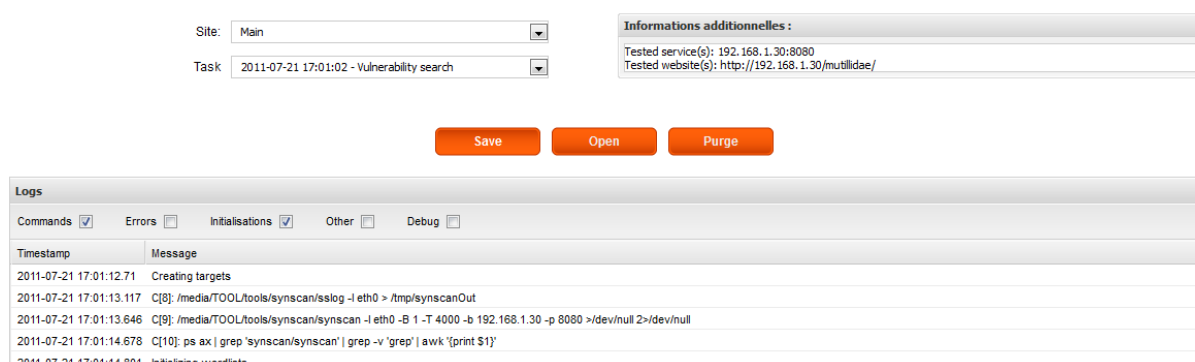
Other Functionalities

View and save audit logs

The audit logs generated by VulnIT can be viewed using the log console (click on the 'Log' link at the top button bar). 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.

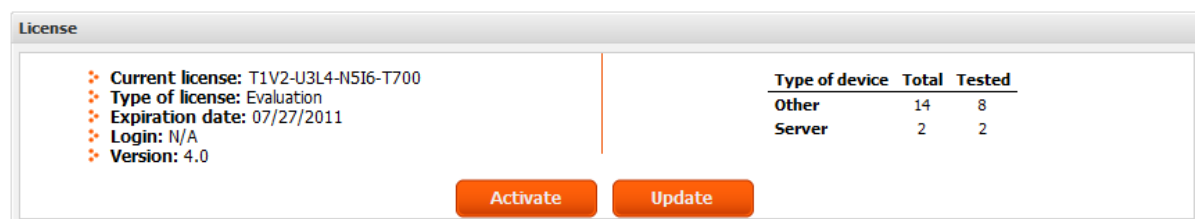
If you wish to keep these logs, click 'Save' at the top of the log console. The save procedure is similar to saving a report (see above).



Finally, if you wish to free some space on the VM, you can delete old logs by clicking on the 'Purge' button.

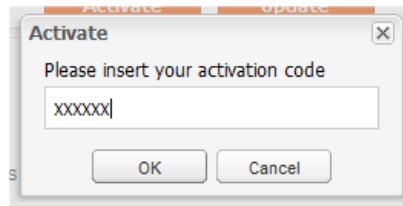
License information

By clicking on the 'About' link at the top right corner of the page, the following screen will appear. This screen displays your license and usage information.



The evaluation license is activated at the first boot and last for two weeks, 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 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.

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'.

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