9. Vulnerability Management

9.1. Scanning

This chapter covers the set up and execution of the actual scans of your systems for vulnerability management. The chapter describes basic first steps. Later sections show the more detailed use and configuration of scan configurations and the analysis of the results.

Generally speaking the GSM may use two different approaches to scan a target:

- Remote Scan
- Authenticated Scan using local security checks

The remote scan is explained in the following sections while the authorized scan is handled in section Authenticated Scan using Local Security Checks. This chapter also covers the differences and advantages of both scan approaches (see section Pros and Cons of Authenticated Scans).

9.1.1. Simple Scan

This first section describes the first steps of the configuration of the first scan. Basically two options are available. The web interface of the GSM appliance, the Greenbone Security Assistant, provides a wizard that creates all required configurations for a first scan with only very little input. Alternatively these configurations can be created manually step by step. The following two sections cover both options. Ideally the individual steps should be followed directly on a GSM appliance.

(_images/gb_movie_icon.png) These steps are also explained in a video based on GOS 3.1 at https://docs.greenbone.net/Videos/gos-3.1/en/GSM-FirstScan-GOS-3.1-en-20150716.mp4 (https://docs.greenbone.net/Videos/gos-3.1/en/GSM-FirstScan-GOS-3.1-en-20150716.mp4).

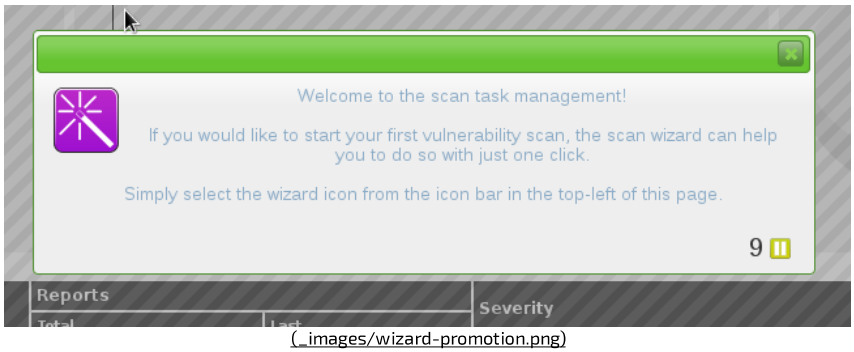
9.1.1.1. Wizard

When logging into the web interface of the GSM appliance for the first time after initial set up the empty dashboard will be displayed.

(_images/emptydashboard.png)

The dashboard is displayed first by default

To configure a new task the admin has to select the menu *Scans* followed by *Tasks*. To ease the setup of the tasks an overlay promoting the wizard will be displayed.



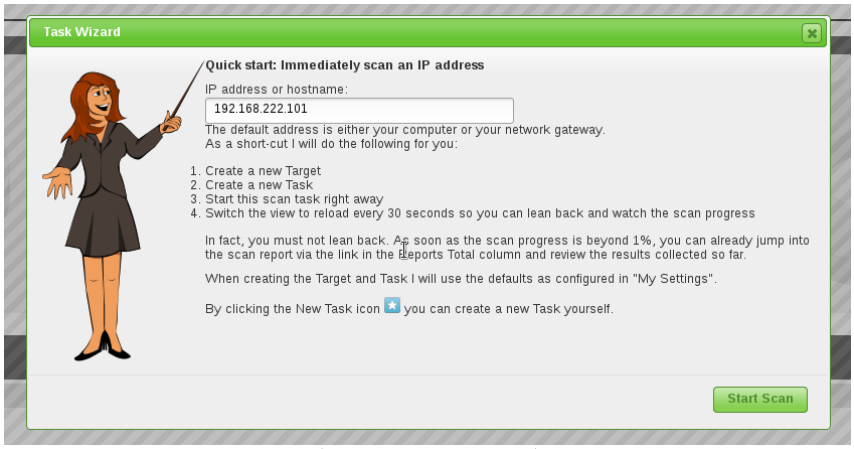
(_images/wizard-promotion.png)

The wizard is promoted using an overlay

By default, this will happen as long as less than four scan tasks were created. The wizard can be started at any time by clicking the (_images/wizard.png) icon in the upper left corner on the screen. Three different options are available:

- Task Wizard
- Advanced Task Wizard
- Modify Task Wizard

To scan a simple system using the wizard first select the *Task Wizard*. For an immediate scan it is enough to enter the IP address or DNS name of the target system. When using a DNS name however, the GSM appliance must be able to resolve the name.



(_images/task-wizard.png)

The task wizard simplifies the first steps

The task wizard then automatically performs the following steps:

1. Creates a new scan target (Target) in the GSM.
2. Creates a new scan task (Task) in the GSM.
3. Starts the scan task immediately.
4. Changes the view and reloads it every 30 seconds in order to monitor the progress of the task.

After the task is started, the progress can be monitored. The Greenbone Security Assistant displays the overview page. The new task can be seen there as well.

(_images/task-fortschritt.png)

After the start, the progress is being displayed.

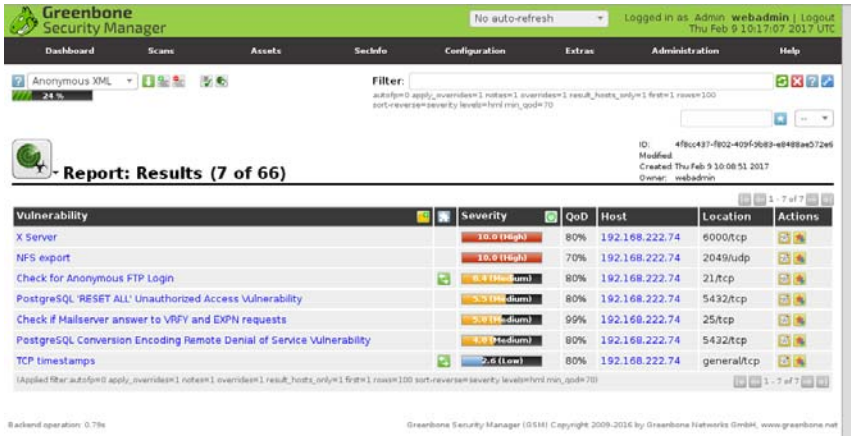
The colour and the fill level of the status bar display the state of the scan (see also section Starting a Task).

The task can be managed via the actions in the right column:

- (_images/start.png) Starting of a currently not running task.
- (_images/stop.png) Stopping of a currently running task. All discovered results will be written to the database.

- (_images/resume.png) Resuming of a stopped task.
- (_images/trashcan.png) Moving of a task to the trashcan.
- (_images/edit.png) Editing of a task.
- (_images/clone.png) Cloning of a task.
- (_images/download.png) Exporting of a task as XML object. The object can be imported again on another GSM.

During the scan and after its completion the admin can view the report by clicking the progress bar. The column Severity displays the criticality of any vulnerabilities found. The prior column Solution Type (_images/solution_type.png) shows the type of any solution available. Usually the most common solution is the VendorFix (_images/st_vendorfix.png).

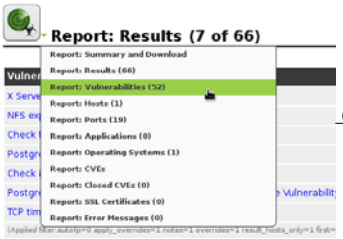


(_images/wizard-result.png)

The results are already available before the scan is completed.

The progress can be continued to be monitored at the top right via the progress bar. This page, however, is not reloaded automatically.

In order to obtain different representations of the results, you can move the mouse over the title bar. It opens a pull-down menu where you can choose different presentations of the results.



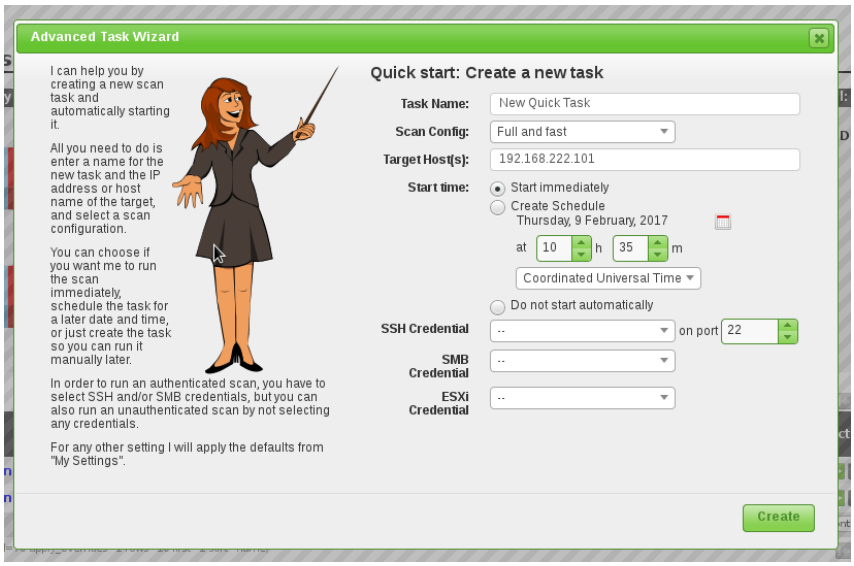
(_images/result-presentations.png)

Furthermore, a report can be displayed using different presentations

Furthermore, the report can be exported in various different formats as well. The export formats are selected in the right column on the Summary and Download view. Afterwards the report can be downloaded by clicking the (_images/download.png) button. Reports and report formats are discussed in more detail in section Reports and Vulnerability Management.

9.1.1.2. Advanced Wizard

Next to the simple wizard the GSM also provides an advanced wizard that allows for more configuration options. This wizard allows for shortcutting the manual configuration of the individual parameters and still allows for a more granular configuration.

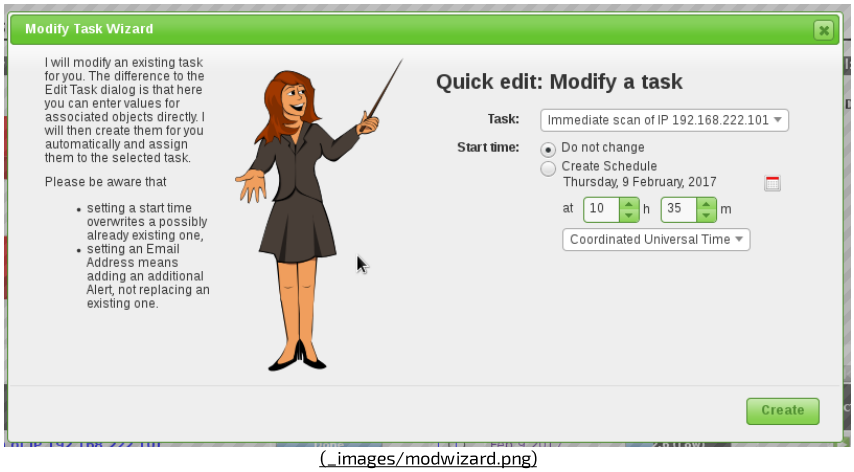


(_images/advwizard.png)

The advanced wizard offers more options.

This wizard can be started by clicking on the wizard icon (_images/wizard.png) in the upper left corner of the task view.

An additional wizard allows the modification of a task (Modify Task Wizard). The task may be renamed and scheduled.



(_images/modwizard.png)

The wizard may be used to schedule an existing task

9.1.1.3. Manual Configuration

The upcoming section covers the creation of a simple scan with its individual steps that the wizard performs as well. This way meaningful names may be selected for both the scan targets (Targets) and the scan task (Task).

(_images/gb_movie_icon.png) These steps are also explained in a video based on GOS 3.1 at https://docs.greenbone.net/Videos/gos-3.1/en/GSM-FirstScan-GOS-3.1-en-20150716.mp4 (https://docs.greenbone.net/Videos/gos-3.1/en/GSM-FirstScan-GOS-3.1-en-20150716.mp4).

9.1.1.3.1. Creating a Target

The first step is to define a scan target. This is called Target by the Greenbone Security Assistant.

First chose one or more systems in your network you want to scan. The IP address or the DNS name is required. In both cases it is necessary that the GSM can connect to the system. When using the DNS name, the GSM appliance must also be able to resolve the name.

(_images/configuration.png)

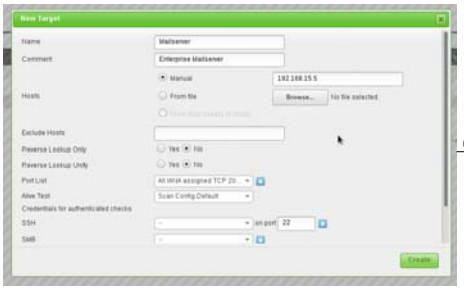
Selecting the target menu.

(_images/newtarget.png)

Targets (2 of 2

Creating a new target.

Choose *Targets* from the menu *Configuration*. Select the *New Target* icon (the white star on blue background: (_images/new.png)) in the upper left corner. This icon is always used to represent the creation of a new object within its respective context.



(_images/newtarget2.png)

Enter the details for the target.

A new overlay, in which the target can be configured in more detail, will open.

Enter the following information:

- **Name**

  The name can be freely chosen. A descriptive name should be chosen if possible. Possibilities are Mailserver, ClientNetwork, Webserverfarm, DMZ or the like, describing the entered systems in more detail.

- **Comment**

  The optional comment allows specifying background information. It simplifies understanding the configured targets later.

- **Hosts**

  Manual entry of the system or importing of a list of systems. When entering manually the following options are available:

  - Single IP address, i.e. 192.168.15.5
  - System name, i.e. mail.example.com
  - IPv4 address range, i.e. 192.168.15.5-192.168.15.27 or 192.168.55.5-27
  - IPv4 network in CIDR notation, i.e. 192.168.15.0/24 [1]
  - Single IPv6 address
  - IPv6 address range in long format, i.e. ::12:fe5:fb50-::12:fe6:100
  - IPv6 address range in short format, i.e. ::13:fe5:fb50-fb80
  - IPv6 address range in CIDR notation, i.e. fe80::222:64ff:fe76:4cea/120
  - multiple entries can be entered separated with commas

  When importing from a file, the same syntax can be used. The entries can be stored in the file on multiple lines. When using long lists of systems to be scanned, this way is usually the simpler one.

  Alternatively the systems may be imported from the host asset database.

- **Exclude Hosts**

  Systems that should be excluded from the lists mentioned above.

- **Reverse Lookup Only**

Only scan IP addresses that can be resolved into a DNS name.

- **Reverse Lookup Unify**
  If multiple IP addresses resolve to the same DNS name the DNS name will only get scanned once.

- **Port list**
  The TCP and UDP protocols support 65535 ports respectively. Scanning all ports in many cases takes too long. Many ports are usually not used. A manufacturer developing a new application often reserves the respective port with the IANA (Internet Assigned Numbers Association). For most scans it is often enough to scan the ports registered with the IANA. But keep in mind that the registered ports differentiate from the privileged ports. Privileged ports are ports smaller than 1024 [2]. But the ports 1433/tcp (MS-SQL) and 3306/tcp (MySQL) are also registered and included in the appropriate lists. Nmap by default uses a different list and doesn't check all ports either. OpenVAS uses a different default as well.

  The scan of TCP ports is usually performed simply and fast. Operating system without firewall features always reply to a TCP request and as such advertise a port as being open (TCP-ACK) or closed (TCP-RST). With UDP this is not the case. The operating system only responds reliably when the port is closed (ICMP-Port-Unreachable). An open port is deducted by the scanner by a missing response. Therefore, the scanner has to wait for an internal timeout. This behaviour is only true for systems not protected by a firewall. When a firewall exists the discovery of open or closed ports is much more difficult.

  If applications run on unusual ports and they should be monitored and tested with the GSM, the default port lists should be verified and adapted using *Configuration* submenu *Port Lists*. If necessary, create your own list that includes your port. A new port list may be directly created using the icon (_images/new.png). The default port lists can not be modified.

- **Alive Test**
  This options specifies the method to check if a target (Targets) is reachable. Options are:
  - ICMP Ping
  - TCP Service Ping
  - ARP Ping
  - ICMP & TCP Service Ping
  - ICMP & ARP Ping
  - TCP Service & ARP Ping
  - ICMP, TCP Service & ARP Ping

In the real world there are problems with this test from time to time. In some environments routers and firewall systems respond to a TCP Service Ping with a TCP-RST even though the host is actually not alive (see also Obstacles while Scanning).

Network components exist that support Proxy-ARP and respond to an ARP-Ping. Therefore this test often requires local customization to your environment.

- **SSH Credential**
  Selection of a user that can log into the target system of a scan if it is a Linux or UNIX system. This allows for an *Authenticated Scan* using local security checks (see section Credentials and Authenticated Scan using Local Security Checks).

- **SMB Credential**
  Selection of a user that can log into the target system of a scan if it is a Microsoft Windows system. This allows for an *Authenticated Scan* using local security checks (see section Credentials and Authenticated Scan using Local Security Checks).

- **ESXi Credential**
  Selection of a user that can log into the target system of a scan if it is a VMWare ESXi system. This allows for an *Authenticated Scan* using local security checks (see section Credentials and Authenticated Scan using Local Security Checks).

- **SNMP Credential**
  Selection of a user that can log into the target system of a scan if it is an SNMP aware system. This allows for an *Authenticated Scan* using local security checks (see section Credentials and Authenticated Scan using Local Security Checks).

All credentials can be created on the fly using the (_images/new.png) icon next to the credential.

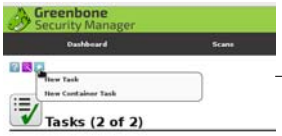
Footnotes

[1] The maximum netmask is /20. This equals 4096 addresses.

[2] In UNIX access to these privileged ports is only allowed for privileged users (i.e. root). Ports starting at 1024 are also available to unprivileged users.

9.1.1.3.2. Creating a Task

The GSM controls the execution of a scan using Tasks. These tasks can be repeated regularly or run at specific times. The scheduling is discussed in more detail in section Scheduled Scan. For now the basic creation of a task is covered in this section.



(_images/newtask.png)

Creation of tasks.

To access the tasks select menu option *Scans* from the menu bar. From there select the *Tasks*. On the following page select the white star (_images/new.png) on blue background to choose *New Task* to create a new task. An overlay opens which can be used to configure the additional options of the task.

(_images/task.png)

Creation of a new task.

The following information can be entered:

- **Name**
  The name can be chosen freely. A descriptive name should be used if possible. Possibilities to describe the entered task are *Scan Mailserver*, *Test ClientNetwork*, *Check DMZ for new ports and systems* or the like.

- **Comment**
  The optional comment allows for the entry of background information. It simplifies understanding the configured task later.

- **Scan Targets**
  Select a previously configured Target from the drop down menu. Additionally, you can create the target on the fly using the (_images/new.png) icon next to the drop down list.

- **Alerts**
  Select a previously configured Alert. Status changes of a task can be communicated to the world via email, Syslog, HTTP or a connector. Additionally, you can create an alert on the fly using the (_images/new.png) icon next to the drop down list.

- **Schedule**
  Select a previously configured Schedule. The task can be run once or repeatedly at a predetermined time. It is possible to scan the network every Monday morning at 6:00 am for example. You can create the schedule on the fly using the (_images/new.png) icon next to the drop down list.

- **Add results to Asset Management**
  Selecting this option will make the systems available to the Asset Management of the GSM automatically (see chapter Asset Management). This selection can be changed at a later point as well.

  - **Apply Overrides**
    Overrides may be directly applied when adding the results to the asset database.

  - **Min QoD**
    Here the minimum quality of detection can be specified for the addition of the results to the asset database.

- **Alterable Task**
  Allow for modification of the task even though reports were already created. The consistency between reports can no longer be guaranteed if tasks are altered.

- **Auto Delete Reports**
  This option may automatically delete old reports. The maximum number of reports to store can be configured. If the maximum is exceeded, the oldest report is automatically deleted. The factory setting is `Do not automatically delete reports` .

- Scanner

- **OpenVAS Scanner**
  By default, only the built-in OpenVAS and the CVE scanning engines are supported. Satellite GSM formerly known as slaves or sensors may be used as additional scanning engines. These need to be configured first using the *Configuration/ Scanners* menu. The following options are only relevant for the OpenVAS scanning engine. The CVE scanner does not support any options.

- **Scan Config**
  The GSM comes by default with seven pre-configured scan configurations for the OpenVAS scanner.

  - **Discovery**
    Only NVTs are used that provide the most possible information of the target system. No vulnerabilities are being detected.

  - **Host Discovery**
    Only NVTs are used that discover target systems. This scan only reports the list of systems discovered.

  - **System Discovery**
    Only NVTs are used that discover target systems including installed operating systems and hardware in use.

  - **Full and Fast**
    This is the default and for many environments the best option to start with. This configuration is based on the information gathered in the prior port scan and uses almost all NVTs. Only NVTs are used that will not damage the target system. Plugins are optimized in the best possible way to keep the potential false negative rate especially low. The other configurations only provide more value only in rare cases but with much more required effort.

  - **Full and fast ultimate**
    This configuration expands the first configuration with NVTs that could disrupt services or systems or even cause shut downs.

  - **Full and very deep**
    This configuration differs from the **Full and Fast** configuration in the results of the port scan and application or service detection not having an impact on the selection of the NVTs. Therefore, NVTs will be used that will have to wait for a timeout or which are testing for vulnerabilities of an application or service which was not detected previously. This scan is very slow.

  - **Full and very deep ultimate**
    This configuration adds the dangerous NVTs that could cause possible service or system disruptions to the **Full and very deep** configuration.

- **Network Source Interface**
  Here you can choose the source interface of the GSM for the scan.

- **Order for target hosts**
  Select how the specified network area should be searched. Options available are:

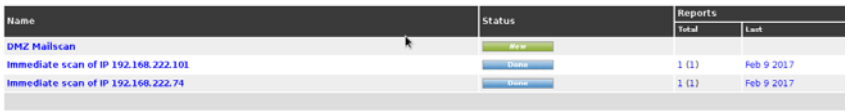
  - Sequential
  - Random
  - Reverse

  This is interesting if for example a network, i.e. 192.168.0.0/24, is being scanned that has lots of systems at the beginning or end of the IP address range. With the selection of the `Random` mode the progress view is more meaningful.

- **Maximum concurrently executed NVTs per host / Maximum concurrently scanned hosts**
  Select the speed of the scan on one host. The default values are chosen sensibly. If more NVTs run simultaneously on a system or more systems are scanned at the same time, the scan might have a negative impact on either the performance of the scanned systems, the network or the GSM appliance itself. These values maxhosts and maxchecks may be tweaked.

9.1.1.3.3. Permissions

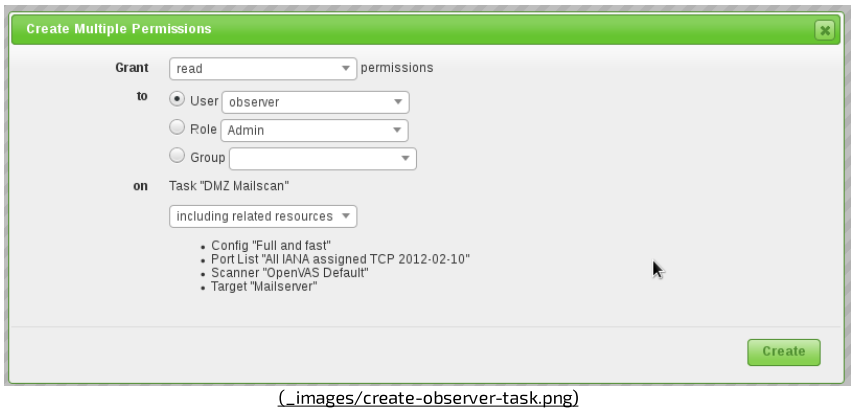
Once the task is saved it will be displayed in the list of scans (see figure A newly created task.).



(_images/neuer-task.png)

A new task once it is created.

Selecting the name of the task using the mouse displays the details of the task. At the bottom of the page the permissions for the task can be managed. To add a permission click the (_images/new.png) icon in the *Permissions* title line.



(_images/create-observer-task.png)

Read permissions can be managed directly in the task.

> **Note**
>
> By default, normal users can not create permissions for other users as they do not have read permission to the user database. To do this a user must specifically have the *get_users* permission. It makes most sense to create an additional role (see section GetUsers Role for Observers (gui_administration.html#getusers-role)).

Select *User*, *Group* or *Role* respectively and enter the respective name. After clicking on *Create* the permissions are created.

This is now displayed in the task overview.

(_images/create-observer-task2.png)

The read permissions of a task are displayed in the overview.

After logging in the user can see those tasks and can access the respective reports.

This is now displayed in the task overview.

(_images/task-uebersicht-observer.png)

After logging in the observer can view the tasks but cannot change them.

9.1.1.3.4. Starting a Task

Once a task is saved it will be displayed in the list of tasks (see figure A newly created task.).

(_images/task-list.png)

A newly created task.

The task can be managed via the action icons in the right column:

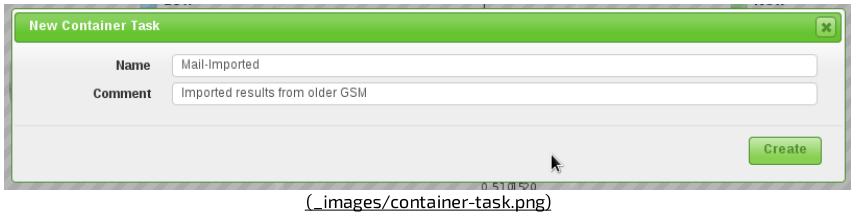
- (_images/start.png) Starting of a currently not running task.
- (_images/stop.png) Stopping of a currently running task. All discovered results will be written to the database.
- (_images/resume.png) Resuming of a stopped task.
- (_images/trashcan.png) Moving of a task to the trashcan.
- (_images/edit.png) Editing of a task.
- (_images/clone.png) Cloning of a task.
- (_images/download.png) Exporting of a task as XML object.

The status bar shows information about the status of a scan. The following colours and states are possible:

- New (_images/status-new.png) The task has not been run since it was created.
- 42 % (_images/status-run.png) The task is currently running and 42% completed. The information is based on the number of NVTs executed on the selected hosts. For this reason the information does not necessarily correlate with the time spent.
- Requested (_images/status-requested.png) The task was just started. The GSM is preparing the scan.
- Delete Requested (_images/status-delete.png) The task was deleted. The actual deletion process can take some time as reports need to be deleted as well.
- Stop Requested (_images/status-stopr.png) The task was stopped recently. However, the scan engine has not reacted respectively yet.
- Stopped at 15 % (_images/status-stop.png) The last scan was stopped by the user at 15%. The latest report is possibly not yet complete. Other reasons for this status could be the reboot of the GSM or a power outage. After restarting the scanner, the task will be resumed automatically.
- Internal Error (_images/status-error.png) An error has occurred. The latest report is possibly not yet complete or is missing completely.
- Done (_images/status-done.png) The task has been completed successfully.
- Container (_images/status-container.png) The task is a container task.

9.1.1.3.5. Container Task

A Container Task can be used to import and provide reports created on other GSMs. To create a container task use the (_images/new.png) icon in the top left corner and choose *New Container Task*. When creating the *Container Task* only the name and a comment may be specified. Afterwards reports may be imported. If several reports are imported they may be compared creating a delta report as well.



(_images/container-task.png)

Container tasks are used to import external reports.

The reports need to be in the GSM XML report format.

9.1.2. Authenticated Scan using Local Security Checks

An authenticated scan may provide more vulnerability details on the scanned system. During an authenticated scan the target is both scanned from the outside via the network and from the inside via a valid user login.

During an authenticated scan the GSM logs in to the target system in order to run these local security checks (LSC). The scan therefore requires the prior setup of user credentials. These credentials are used to authenticate to different services on the target system. In some circumstances the results could be limited by the permissions of the users used.

The NVTs in the corresponding NVT families (local security checks) will only be executed if the GSM was able to log in to the target system. The local security check NVTs in the resulting scan are minimally invasive.

The GSM only determines the risk level but does not introduce any changes on the target system. However, the login by the GSM is probably being logged in the protocols of the target system.

The GSM can use different credentials based on the nature of the target. However, the most important ones are:

- SMB

  On Windows systems the GSM can check the patch level and locally installed software such as Adobe Acrobat Reader or the Java suite.

- SSH
  This access is used to check the patch level on UNIX and Linux systems.

- ESXi
  This access is used for testing of VMWare ESXi servers locally.

- SNMP
  Network components like routers and switches may be tested via SNMP.

9.1.2.1. Pros and Cons of Authenticated Scans

The extent and success of the testing routines for authenticated scans depend heavily on the permissions of the account used. On Linux systems an unprivileged user is sufficient and may access most interesting information while especially on Windows systems unprivileged users are very restricted and administrative users provide more results. An unprivileged user does not have access to the Windows registry, the Windows system folder `\windows` , which contains the information on updates and patchlevels, etc.

Local security checks are the most gentle method to scan for vulnerability details. While remote security checks try to be least invasive as well, they might have some impact.

Simply stated an authenticated scan is similar to a Whitebox approach. The GSM has access to prior information and may access the target from within. Especially the registry, software versions and patchlevel are accessible.

A remote scan is similar to a Blackbox approach. Here the GSM uses the same techniques and protocols as a potential attacker to access the target from the outside. The only information available was collected by the GSM itself. During the test the GSM may provoke malfunctions to extract any available information on the used software. The scanner might for example send a malformed request to a service to trigger a response containing further information on the deployed product.

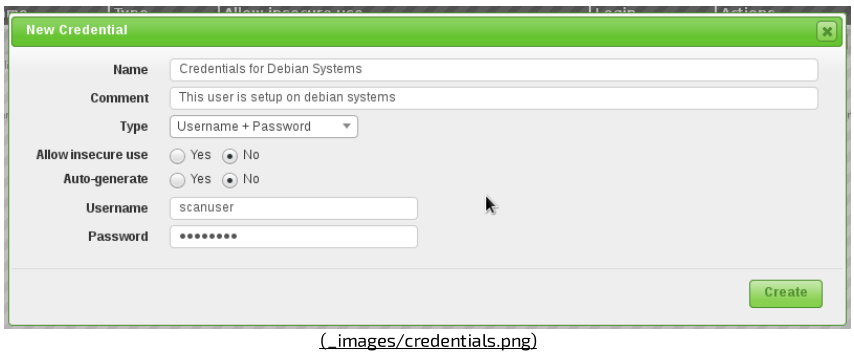
During a remote scan using the scan configuration `Full and Fast` all remote checks are safe. The used NVTs might have some invasive components but none of the used NVTs try to trigger a defect of malfunction in the target (see example below). This is ensured by the scan preference `safe_checks=yes` in the scan configuration. All NVTs with very invasive components or which might trigger a denial of service (DoS) are automatically excluded from the test.

9.1.2.1.1. Example of an invasive NVT

An example for an invasive but safe NVT is the Heartbleed NVT. This is executed even with `safe_checks` enabled because the NVT does not have any negative impact on the target. But the NVT is still invasive because it does test the memory leakage of the target. If the target is vulnerable, actual memory of the target is leaked. The GSM does not evaluate the leaked information but just the fact that the memory was leaked. The information is immediately discarded.

9.1.2.2. Credentials

To access the credentials select the submenu *Credentials* from the *Configuration* menu. To create new credentials use the (_images/new.png) icon in th upper left corner. An overlay is displayed where the following information can be entered:



(_images/credentials.png)

SSH keys can be utilized with credentials as well.

- Name
  An arbitrary name for the credentials.

- Comment
  A freely selectable comment.

- Type
  The following types may be chosen:

  - Username + Password
  - Username + SSH Key

    - Client Certificate
    - SNMP

- **Allow insecure use**
  The GSM will only use the credentials using encrypted protocols by default.

- **Autogenerate Credentials**
  The GSM itself is creating a random password.

- **Username**
  The login name used by the GSM to authenticate on the scanned target system.

- **Password**
  The password can be entered.

Depending on the Type further options might be shown:

- SSH

  - **Private Key**
    If authentication is performed via SSH the private key can be uploaded.

  - **Passphrase**
    If required, the passphrase of the private SSH key can be entered.

- Client Certificate

  - **Certificate**
    If authentication is performed via a client certificate the certificate file may be uploaded.

  - **Private Key**
    The corresponding private key can be uploaded.

- SNMP

  - **SNMP Community**
    If the protocols SNMPv1 or SNMPv2c are used the community can be entered.

  - **Username**
    For SNMPv3 the username may be specified.

  - **Password**
    For SNMPv3 the password may be specified.

  - **Privacy password**
    For SNMPv3 the password for the encryption may be specified.

  - **Auth algorithm**
    The authentication algorithm may be chosen. Supported are either MD5 or SHA1.

  - **Privacy algorithm**
    The encryption algorithm may be chosen. Supported are AES128, DES or none.

9.1.2.2.1. Autogenerate Credentials

To simplify the installation and creation of accounts for authenticated scans the GSM option *Autogenerate Credential* offers an installation package for the respective target system. This package creates the user and the most important permissions for the authenticated scan and re-sets them again during uninstallation.

The installation package is provided for:

- Debian based systems (_images/deb.png)

- RPM based systems (_images/rpm.png)
- Windows (_images/exe.png)
- Public Key (_images/key.png)

9.1.2.3. Requirements on Target Systems with Windows

9.1.2.3.1. General notes on configuration

- The remote registry service must be started in order to access the registry

  You can achieve this by configuring the service to automatically start up. If you do not prefer the automatic start, you could configure manual start up. In that case the service will be started while the system is scanned by GSM and afterwards it will be disabled again. To ensure this behaviour the following item about LocalAccountTokenFilterPolicy must be considered.

- It is necessary that for all scanned systems the file and printer sharing is activated. When using Windows XP, take care to disable the setting "Use Simple File Sharing".
- For individual systems not attached to a domain the following registry key must be set:

  ```
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
  DWORD: LocalAccountTokenFilterPolicy = 1
  ```

- On systems with domain controller the user account in use must be a member of the group **Domain Administrators** to achieve the best possible results. Due to the permission concept it is not possible to discover all vulnerabilities using the **Local Administrator** or the administrators assigned by the domain. Alternatively follow the instructions below under Configuring a domain account for authenticated scans.
- Should a **Local Administrator** be selected – which we explicitly do not recommend – it is mandatory to set the following registry key as well:

  ```
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
  DWORD: LocalAccountTokenFilterPolicy = 1
  ```

- Generated install package for credentials: The installer sets the `Remote Registry` service to auto start. If the installer is executed on a Domain Controller, the user account will be assigned to the Group **BUILTIN/Administrators** (`SID S-1-5-32-544`).
- An exception rule for the GSM on the Windows firewall must be created. Additionally, on XP systems the **File and Printer Sharing** must be set to `enabled` .
- Generated install package for credentials: During the installation the installer offers a dialog to enter the IP address of the GSM. If the entry is confirmed, the firewall rule is configured. The **File and Printer Sharing** service will be enabled in the firewall rules.

9.1.2.3.2. Configuring a domain account for authenticated scans

In order to use a domain account for host based remote audits on a windows target this must be performed under Windows XP Professional, Windows Vista, Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 7, Windows 8, Windows 8.1 or Windows 10 and also be part of a domain.

Taking security into consideration the following eight steps should be implemented to create these scans.

9.1.2.3.2.1. Step 1: Create a security group

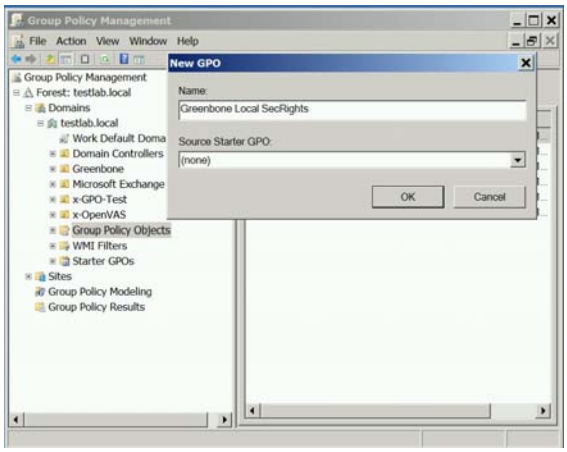
First create a security group called `Greenbone Local Scan` :

- Log into a domain controller and open `Active Directory Users and Computers` .
- Now create the security group in the menu. Select Action > New > Group.
- Call the group `Greenbone Local Scan` . It is important that the Global is selected for the Group Scope and Security as the Group Type.
- Add the account, that is being used for the local authenticated scans under Windows by the Greenbone Appliance, to the group `Greenbone Local Scan` .

9.1.2.3.2.2. Step 2: Create a Group Policy

Now create a group policy with called `Greenbone Local SecRights` .

- Open the Group Policy Management console.
- Right-click on Group Policy Objects and select New.
- Enter `Greenbone Local SecRights` as the name of the policy.



(_images/win_group_policy.png)

A new Windows Group Policy Object for Greenbone scans.

9.1.2.3.2.3. Step 3: Configuration of the Policy

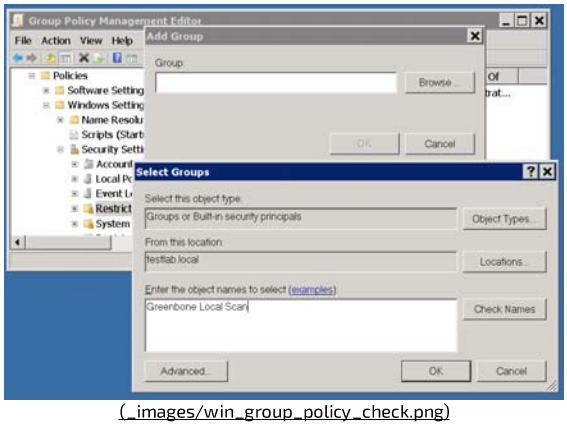
Add the group `Greenbone Local Scan` to the `Greenbone Local SecRIghts` policy and insert local administrators to the groups.

Please note that this setting still exists after the GPO has been removed (*Tattooing GPO*). This changes fundamental privileges which might not be simply reversed by removing the GPO. Please research first whether these settings are compatible with your environment!

- Click on the policy `Greenbone Local SecRights` and select `Edit` .
- Open:

```
Computer Configuration\Policies\Windows Settings\
Security Settings\Restricted Groups
```

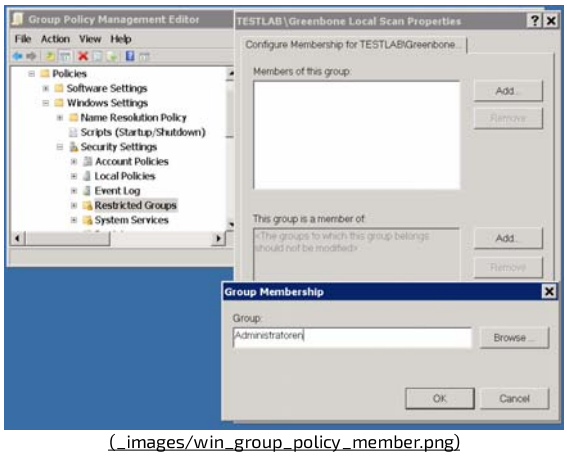
- In the left pane right click on Restricted Groups and select `Add Group`
- Now select `Browse` in the `Add Group` dialog, enter `Greenbone Local Scan` , afterwards click `Check Names` .



(_images/win_group_policy_check.png)

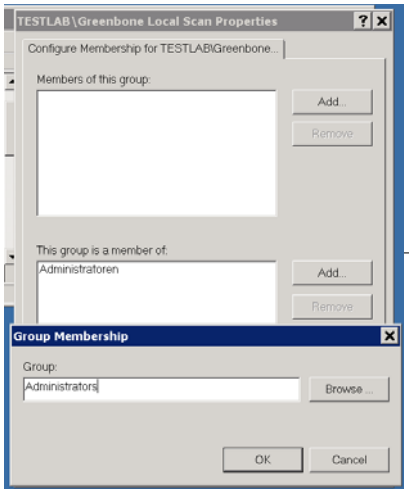
Check Windows Group Name.

- Click OK twice to close the opened dialog.
- Under `This group is member of:` click on `Add` .
- Add the group `Administrators` . Additionally, on non-English systems enter the respective name of the local administrator group.



(_images/win_group_policy_member.png)

Add Group Membership.



(_images/win_group_policy_member2.png)

Add another Group Membership.

- Click OK twice.

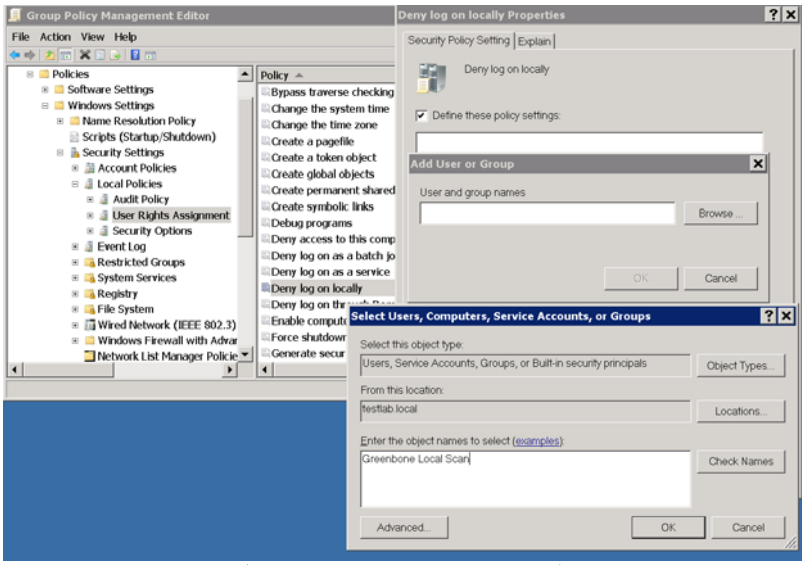
Step 4: Configuration of the policy, to deny local log on systems of the `Greenbone Local Scan` group

Add the `Greenbone Local Scan` to the `Greenbone Local SecRights` group and deny the local log in of group members.

- Click on the `Greenbone Local SecRights` and then select `Edit` .
- Open:

```
Computer Configuration\Policies\Windows Settings\Security Settings\
Local Policies\User Rights Assignment
```

- In the right pane double-click on `Deny log on locally`
- Set the checkmark in `Define these policy settings:`
- Click on `Add User or Group`
- Now select `Browse` , enter `Greenbone Local Scan` and then click on `Check Names` .



(_images/win_group_policy_deny.png)

Edit the policy for local log on.

- Now click twice on OK to close the opened dialog.
- Click OK.

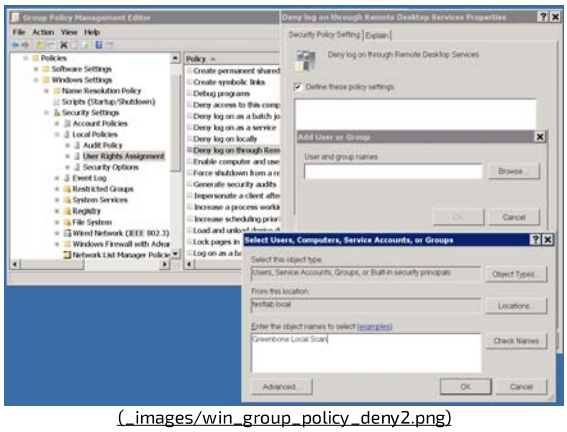
Step 5: Configure the policy to deny the group `Greenbone Local Scan` logging into systems remotely

Add the `Greenbone Local Scan` to the `Greenbone Local SecRights` group and deny group members logging in via RDP.

- Click the policy `Greenbone Local SecRights` and then select `Edit` .
- Open:

```
Computer Configuration\Polices\Windows Settings\Security Settings\
Local Policies\User Rights Assignment
```

- In the right pane double-click on `Deny log on through Remote Desktop Services` .
- Set the checkmark in `Define these policy settings:`
- Click on `Add User or Group`
- Now select `Browse` in the dialog, enter `Greenbone Local Scan` , then click on `Check Names` .



(_images/win_group_policy_deny2.png)

Edit Policy for remote log in.

- Now click twice on OK to close the opened dialog.
- Click OK.

Step 6 (Optional): Configure the policy to give only read permissions to the local drive for the `Greenbone Local Scan` group.

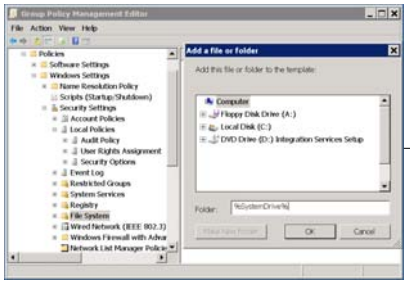
Restrict the permissions to the system drive in the `Greenbone Local SecRights` policy for the `Greenbone Local Scan` group. Please note that this setting still exists after the GPO has been removed (`Tattooing GPO`). This changes fundamental privileges which might not be simply reversed by removing the GPO. Please research first whether these settings are compatible with your environment!

- Click on the `Greenbone Local Sec Rights` policy and then select `Edit` .

- Open:

```
Computer Configuration\Polices\Windows Settings\Security Settings\File Systems
```

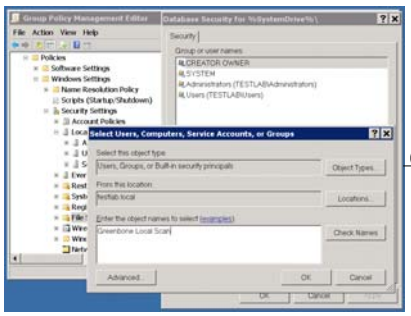
- In the left pane right click on File System and select `Add File…` .
- In the Folder field enter: `%SystemDrive%` and click OK.



(_images/win_group_policy_read.png)

Specifying the `%SystemDrive%` folder.

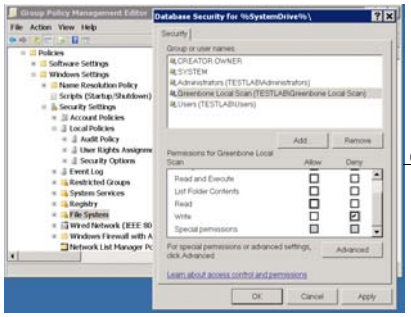
- Click on Add under `Group or user names:`
- In the dialog that opens enter `Greenbone Local Scan` and click OK.



(_images/win_group_policy_read2.png)

Select the `Greenbone Local Scan` group.

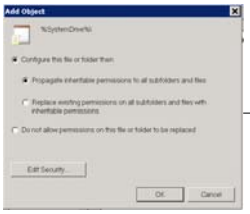
- Now select the user `Greenbone Local Scan` .
- Deactivate all checkmarks under `Allow` and activate the checkmarks under Deny > Write.



(_images/win_group_policy_read3.png)

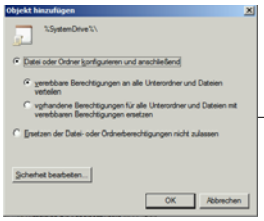
Deny Write access to the group.

- Afterwards click on OK and confirm the warning message with `Yes` .
- Now select `Configure this file or folder then` and `Propagate inheritable permissions to all subfolders and files` and then click on OK.



(_images/win_group_policy_read4.png)

Make the permissions recursive.



(_images/win_group_policy_read4-de.png)

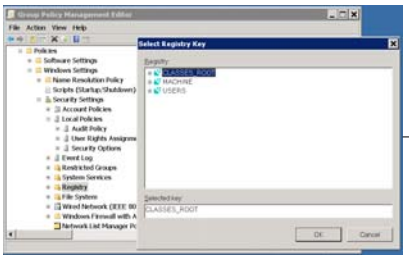
Policy for read permissions on the system drive.

Step 7 (Optional): Configure the policy to give only read permissions to the registry for the `Greenbone Local Scan` group.

To achieve complete restriction is very difficult and possible with a lot of effort. If necessary, critical branches can be secured additionally by adding the branches manually.

Please note that this setting still exists after the GPO has been removed (*Tattooing GPO*). This changes fundamental privileges which might not be simply reversed by removing the GPO. Please research first whether these settings are compatible with your environment!

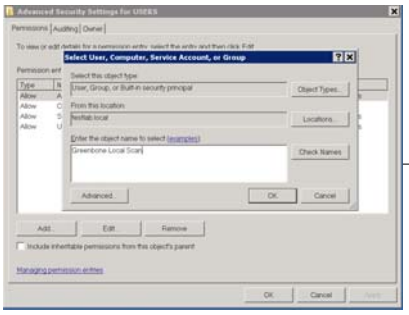
- In the left pane right click `Registry` and select `Add Key` .
- Select `Users` and click OK



(_images/win_group_policy_reg.png)

Select the `USERS` registry key.

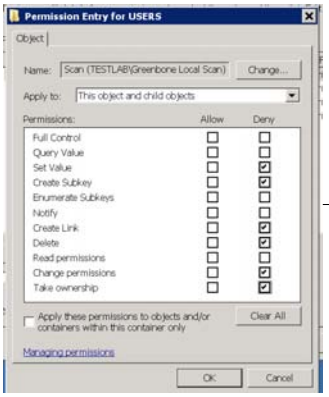
- Click on Advanced and then Add.
- Enter `Greenbone Local Scan` in the dialog that opens and click on OK.



(_images/win_group_policy_reg2.png)

Select the `Greenbone Local Scan` group.

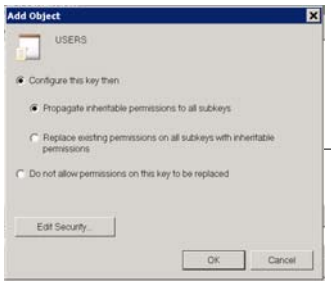
- In the following dialog select for `Apply to: This object and child objects`
- Under Permissions select Deny for `Set Value` , `Create Subkey` , `Create Link` , `Delete` , `Change Permissions` and `Take Ownership` .



(_images/win_group_policy_reg3.png)

Disallow edition of the registry.

- Do not select anything under `Allow` !
- Afterwards click OK twice and confirm the warning message with `Yes` .
- Click OK again.
- Now select `Configure this key then` and `Propagate inheritable permissions to all subkeys` and then click OK.



(_images/win_group_policy_reg4.png)

Propagate the new settings recursively.

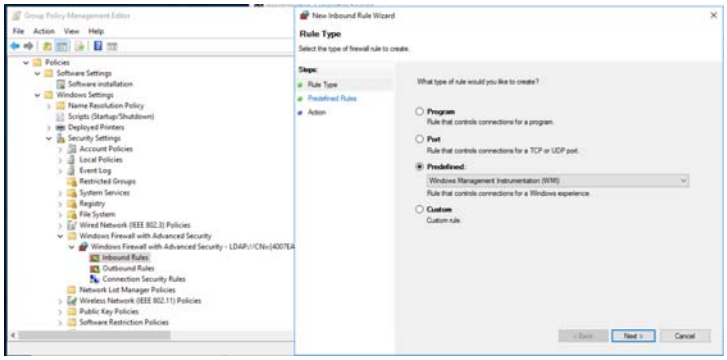
- Repeat the above mentioned steps also for MACHINE and CLASSES_ROOT by clicking on Registry in the right pane and then select `Add key...` .

9.1.2.3.2.4. Step 8 (Optional): Allow WMI access on Windows Vista, 7, 8, 10, 2008, 2008R2, 2012 and 2016 Windows Firewall

- Click on the `Greenbone Local Sec Rights` policy and then select `Edit` .
- Open:

```
Computer configuration\Policies\Windows Settings\Security
Settings\Windows Firewall with Advanced Security\Windows Firewall with
Advanced Security\Inbound Rules
```

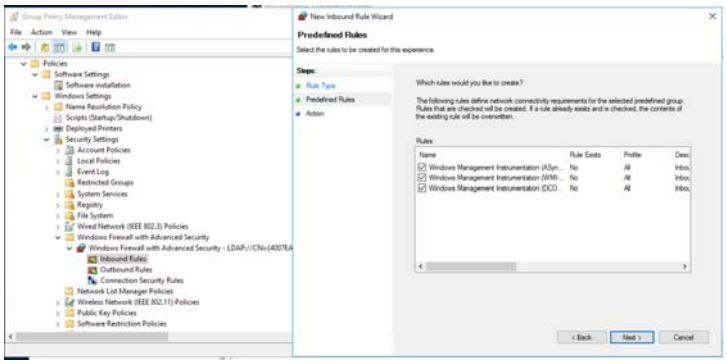
- Right mouse click in the working area and choose New Rule...?
- Choose the Predefined option, and click on Windows Management Instrumentation (WMI) from the drop-down list.



(_images/win_group_policy_fw.png)

Configuring the firewall via GPO

- Click on Next.
- Click the check boxes for:
  - Windows Management Instrumentation (ASync-In)
  - Windows Management Instrumentation (WMI-In)
  - Windows Management Instrumentation (DCOM-In)



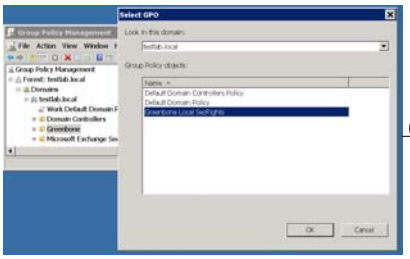
(_images/win_group_policy_fw1.png)

Configuring the firewall via GPO

- Click on Next.
- Click on Finish.

9.1.2.3.2.5. Step 9: Linking of the Group Policy Object

- On the right pane in the Group Policy Management console right click on the domain or Organizational Unit `Link an Existing GPO` and select `Link an Existing GPO…` .
- Now select the group policy object `Greenbone Local SecRights` . The values shown in the figure only serve as example.



(_images/win_group_policy_link.png)

Linking the policy.

9.1.2.3.2.6. Restrictions

Based on the fact that write permissions to the registry and system drive have been removed, the following two tests will no longer work:

- **`Leave information on scanned Windows hosts`** OID 1.3.6.1.4.1.25623.1.0.96171

  This test, if desired, creates information about the start and end of a scan under HKLMSoftwareVulScanInfo. Due to denying write access to HKLM this is no longer possible. If you continue to desire this, the GPO must be adjusted here respectively.

- **`Windows file Checksums`** OID 1.3.6.1.4.1.25623.1.0.96180

  This test, if desired, when executed saves the tool ReHash under C:\Windows\system32 (for 32-bit systems) or c:\Windows\SysWOW64 (for 64-bit systems). Due to denying write access this is no longer possible. The tool must be saved separately or the GPO must be adjusted respectively.

  More information can be found in section File Checksums (compliance.html#compliance-file-checksums).

9.1.2.3.3. Scanning without domain admin and local admin permissions

Theoretically it is possible to build a GPO in which the user also does not have any local admin permissions. But the effort to add respective read permissions to each registry branch and folder as well, is enormous. Unfortunately inheriting of permissions is deactivated for many folders and branches. Additionally, these changes can be set by GPO but cannot be removed again (Tattooing GPO). Also, specific permissions could be overwritten so that additional problems could occur.

To go this route does not make a lot of sense from a technical and administrative perspective.

9.1.2.4. Requirements on Target Systems with Linux/UNIX

- For authenticated scans on Linux or UNIX systems regular user access is usually enough. The login is performed via SSH. The authentication is done either with passwords or an SSH key stored on the GSM.
- Generated installation package for credentials: The install package for Linux Debian or Linux RedHat is a `.deb` or a `.rpm` respectively, creating a new user without any specific permissions. An SSH Key that is created on the GSM is stored in the users home folder. For users of other Linux distributions or UNIX derivatives the key is offered for download. The creation of a user and

saving the key with the proper file permissions is the responsibility of the user.

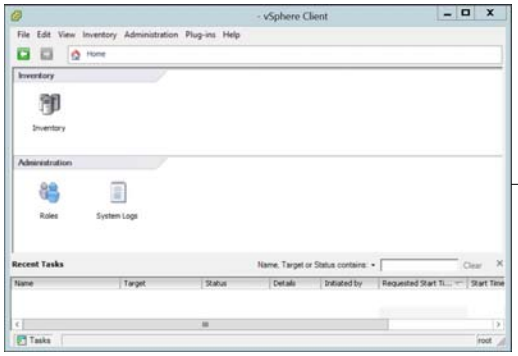
- In both cases it needs to be made sure that Public Key authentication is not prohibited by the SSH daemon. The line `PubkeyAuthentication no` can not be present.
- Already existing SSH keys protected by an optional passphrase can be used as well. It is recommended to use the RSA and DSA formats as created by the command **ssh-keygen**.
- For scans that include policy testing root permission or the membership in specific groups (often `wheel`) might be necessary. For security reasons many configuration files are only readable by super user or members of specific groups.

9.1.2.5. Requirements on Target Systems with ESXi

By default, local ESXi users are limited to read-only roles. Either an administrative account or a read-only role with permission to global settings must be used.

The following steps will guide you through the process.

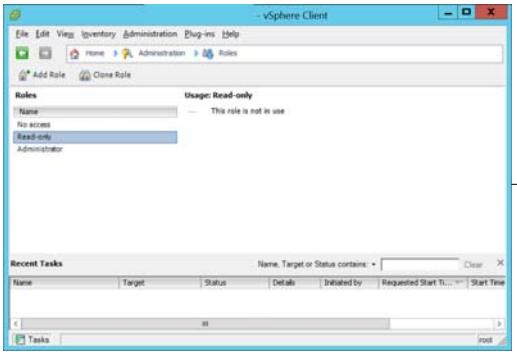
Start the Vsphere client.



(_images/vsphere1.png)

The vsphere client offers access to the roles.

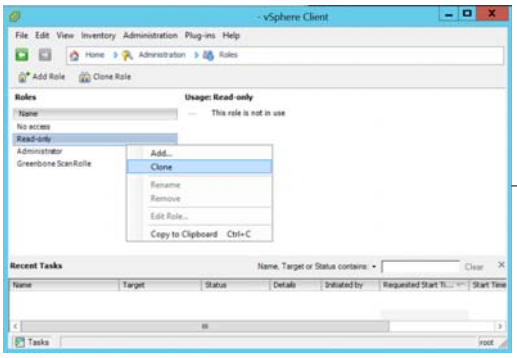
On the Home screen click `Roles` .



(_images/vsphere2.png)

The roles are displayed.

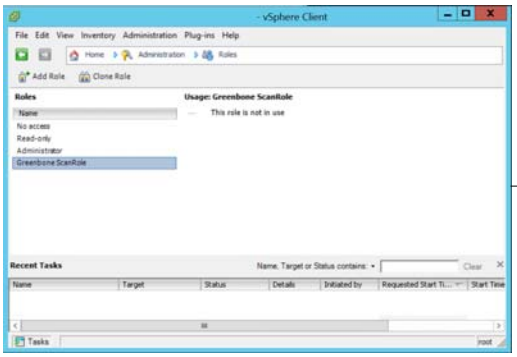
Select the Role `ReadOnly` by right-clicking with the mouse. Clone the role. The list will now contain the Clone as well.



(_images/vsphere3.png)

The clone is added.

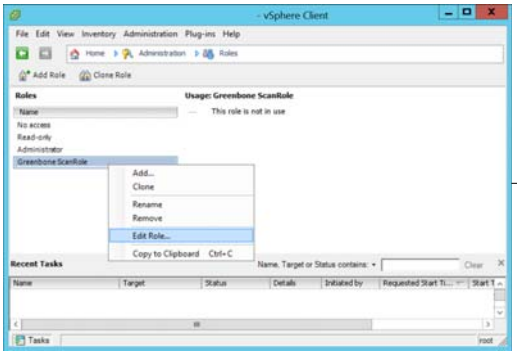
Rename the cloned role appropriately. In this case `Greenbone Scan Role` is used.



(_images/vsphere4.png)

The clone may be renamed.

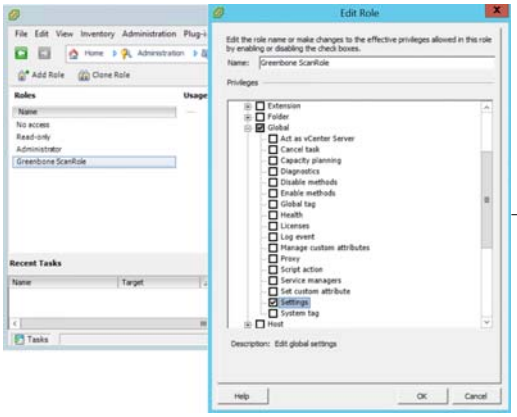
Now modify the new role by right-clicking the role again with the mouse



(_images/vsphere5.png)

Modify the new Greenbone role.

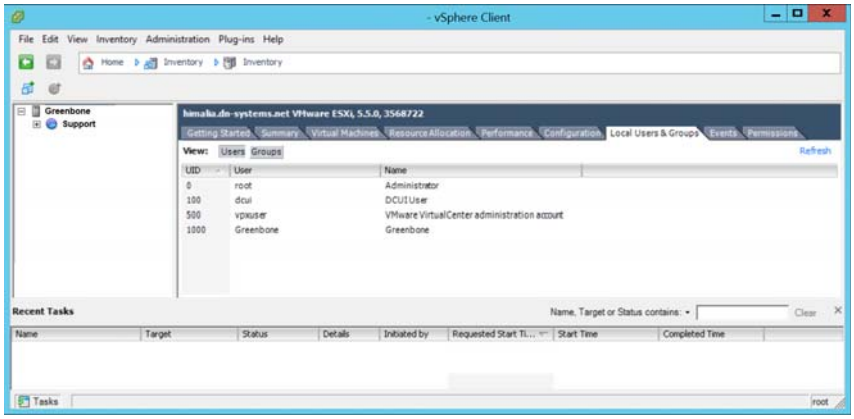
Add the privilege `Global > Settings` to the role.



(_images/vsphere6.png)

Add Global>Settings to the role.

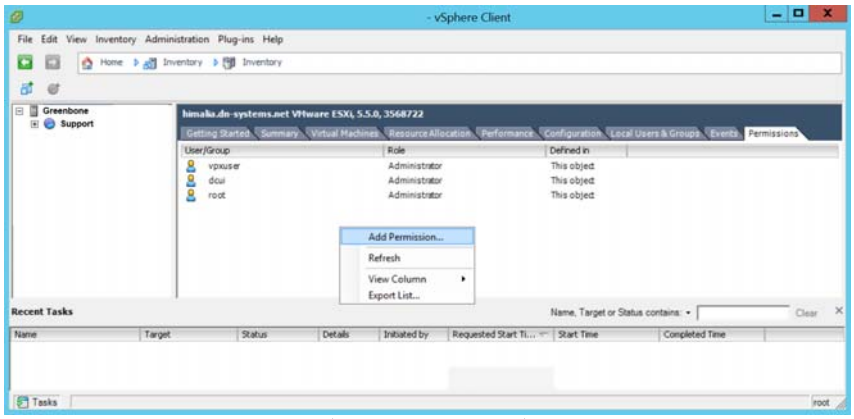
Finally, assign the new role to the scan user account used by the GSM. Choose the appropriate user from the list of local users and groups.



(_images/vsphere7.png)

Access the list of local users.

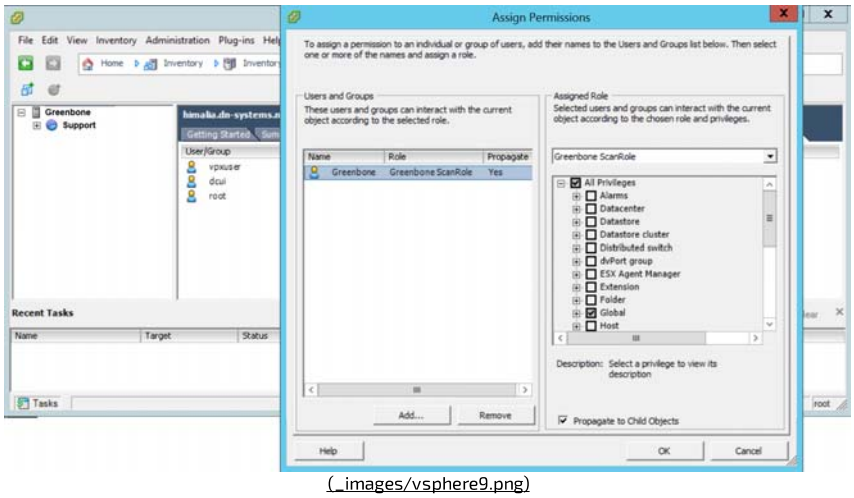
Go to the permissions tab and click the empty space. Choose `Add Permission` .



(_images/vsphere8.png)

Add a permission on the privileges tab.

Select the created role in the right column. Add the appropriate user in the left column and apply the change using the `OK` Button.



(_images/vsphere9.png)

Assign the role to the user.

9.1.2.6. Requirements on Target Systems with Cisco OS

The GSM may check network components like routers and switches for vulnerabilities as well. While the usual network services are discovered and checked via the network some vulnerabilities may only be discovered by an authenticated Scan. For the authenticated scan the GSM may use either SNMP or SSH. This section will cover both approaches.

9.1.2.6.1. SNMP

The GSM may use the SNMP protocol to access the Cisco network component. The GSM support SNMPv1, v2c and v3. SNMP uses the port 161/udp. The default port list does not include any UDP port. Therefore, this port is ignored during the vulnerability test using `Full and Fast` and no SNMP check is enabled. To scan network components the port list should be modified to include at least the following ports:

- 22/tcp SSH
- 80/tcp 8080/tcp HTTP
- 443/tcp 8443/tcp HTTPS
- 2000/tcp SCCP
- 2443/tcp SCCPS
- 5060/tcp 5060/udp SIP
- 5061/tcp 5061/udp SIPS
- 67/udp DHCP Server
- 69/udp TFTP
- 123/udp NTP
- 161/udp SNMP

- 162/udp SNMP Traps
- 500/udp IKE
- 514/udp Syslog
- 546/udp DHCPv6
- 6161/udp 6162/udp Unified CM

The admin might want to set up special port list to be used just for such network components.

The GSM needs to access only very few objects from the SNMP tree. For least privilege access an SNMP view should be used to constrain the visibility of the SNMP tree for the GSM. The following two examples explain how to set up the view using either a community string or an SNMPv3 user.

To use an SNMP community string the following commands are required on the target:

```
# configure terminal
```

Using an access list the usage of the community may be restricted. The IP address of the GSM is 192.168.222.74 in this example:

```
(config) # access-list 99 permit 192.168.222.74
```

The view `gsm` should only allow accessing the system description:

```
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```

The last command links the community `gsm-community` with the view `gsm` and the access-list 99:

```
(config) # snmp-server community gsm-community view gsm RO 99
```

When using an SNMPv3 user including encryption the following configuration lines are required on the target:

```
# configure terminal
(config) # access-list 99 permit 192.168.222.74
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```

SNMPv3 requires the setup of a group first. Here the group `gsmgroup` is linked to the view `gsm` and the access-list 99:

```
(config) # snmp-server group gsmgroup v3 priv read gsm access 99
```

Now the user may be created supplying the password `gsm-password` and the encryption key `gsm-encrypt`. The authentication is done using md5 while the encryption is handled by AES128:

```
(config) # snmp-server user gsm-user gsm-group v3 auth md5 gsm-password priv aes 128 gsm-encrypt
```

To configure either the community or the SNMPv3 user in the GSM the admin uses *Configuration/ Credentials* (see section Credentials).

9.1.2.6.2. SSH

The authenticated scan may be performed via SSH as well. When using SSH, the usage of a special unprivileged user is recommended. The GSM currently only requires the command `show version` to retrieve the current version of the firmware of the device.

To set up a least privilege user which is only able to run this command several approaches are possible. The following example uses the Role-Based-Access-Control feature.

> **Tip**
>
> Before using the following example, make sure you understand all side effects of the configuration. If used without verification the system may restrict further logins via SSH or Console.

To use role based access control AAA and views have to be enabled:

```
> enable
# configure terminal
(config)# aaa new-model
(config)# exit
> enable view
# configure terminal
```

The following lines create a restricted view including just the command `show version`. The supplied password `view-pw` is not critical:

```
(config)# parser view gsm-view
(config-view)# secret 0 view-pw
(config-view)# commands exec include show version
(config-view)# exit
```

Now the user `gsm-user` with the password `gsm-pw` is created and linked to the view `gsm-view` :

```
(config)# username gsm-user view gsm-view password 0 gsm-pw
(config)# aaa authorization console
(config)# aaa authorization exec default local
```

If SSH is not yet enabled the following lines take care of that. Use the appropriate hostname and domain:

```
(config)# hostname switch
(config)# ip domain-name greenbone.net
(config)# crypto key generate rsa general-keys modulus 2048
```

Finally, enable SSH logins using the following commands:

```
(config)# line vty 0 4
(config-line)# transport input ssh
(config-line)# Crtl-Z
```

Now the credentials of the user need to be entered on the GSM. Navigate to *Configuration* followed by *Credentials* and create the appropriate user. Then link the credentials to the target to be used as SSH-credentials.

9.2. Scan Configuration

The GSM appliance comes with various pre-defined scan configurations. However, they can be customized and expanded by your on configurations. The following configurations are already available from Greenbone:

Empty

This is an empty template.

Discovery

Only NVTs are used that provide information of the target system. No vulnerabilities are being detected.

Host Discovery

Only NVTs are used that discover target systems. This scan only reports the list of systems discovered.

System Discovery

Only NVTs are used that discover target systems including installed operating systems and hardware in use.

Full and Fast

For many environments this is the best option to start with. This configuration is based on the information gathered in the prior port scan and uses almost all plugins. Only plugins are used that will not damage the target system. Plugins are optimized in the best possible way to keep the potential false negative rate especially low. The other configurations only provide more value only in rare cases but with much more required effort.

Full and fast ultimate

This configuration expands the **Full and Fast** configuration with plugins that could disrupt services or systems or even cause shutdowns.

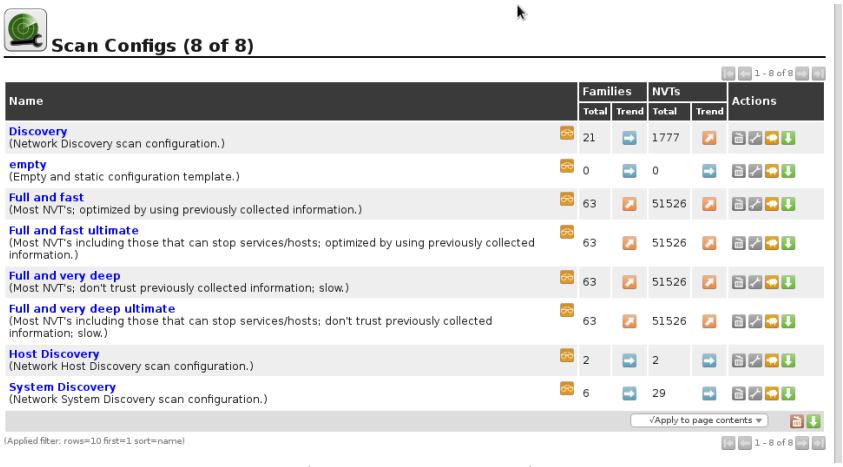
Full and very deep

This configuration differs from the **Full and Fast** configuration in the results of the port scan and application or service detection not having an impact on the selection of the plugins. Therefore, plugins will be used that will have to wait for a timeout or which are testing for vulnerabilities of an application or service which was not detected previously. This scan is very slow.

Full and very deep ultimate

This configuration adds the dangerous plugins that could cause possible service or system disruptions to the **Full and very deep** configuration. This scan is also very slow.

The available scan configurations can be viewed under *Configuration/ Scan Configs*. Remember that by default only the first 10 configurations are always displayed.



(_images/scan-configs.png)

The GSM comes with various scan configurations.

In figure The GSM comes with various scan configurations, one can identify how many NVT families and how many NVTs are activated in a configuration. Additionally, it shows the trend if a scan configuration was configured dynamically (_images/trend_more.png) or statically (_images/trend_nochange.png).

Greenbone publishes new plugins regularly (NVTs). Also, new NVT families can be introduced through the Greenbone Security Feed.

- (_images/trend_more.png) dynamic

  > Scan configurations that are configured dynamically will include and activate new NVT families and new NVTs of the respective activated families automatically after a NVT Feed update. This ensures that new NVTs are available immediately and without any interaction by the administrator.

- (_images/trend_nochange.png) static

  > Scan configurations that are configured statically will not change after an NVT Feed update.

The (_images/view_other.png) icon indicates if the scan configuration is available to and can be used by other users.

(_images/local-scan-config.png)

User's scan configurations are only visible to them.

To make a configuration available the respective user, role or group must be assigned the *get_configs* permission. Then this configuration will be visible to the respective users as well.

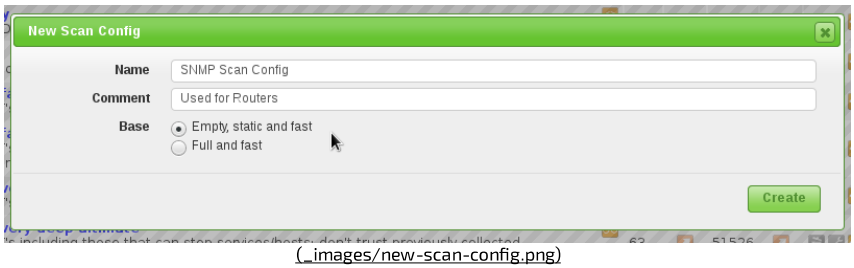
(_images/config-owned.png)

With the appropriate permissions other users can use the configuration.

9.2.1. Creating a New Scan Configuration

To create a new scan configuration first select *Configuration/ Scan Configs*. Then by clicking on (_images/new.png) in the upper left corner a new scan configuration can be created.

Alternatively a scan configuration can be imported using the (_images/upload.png) icon. Greenbone themselves offer different scan configurations on their website. In addition, scan configurations can be exported on other GSM appliances and then imported.



(_images/new-scan-config.png)

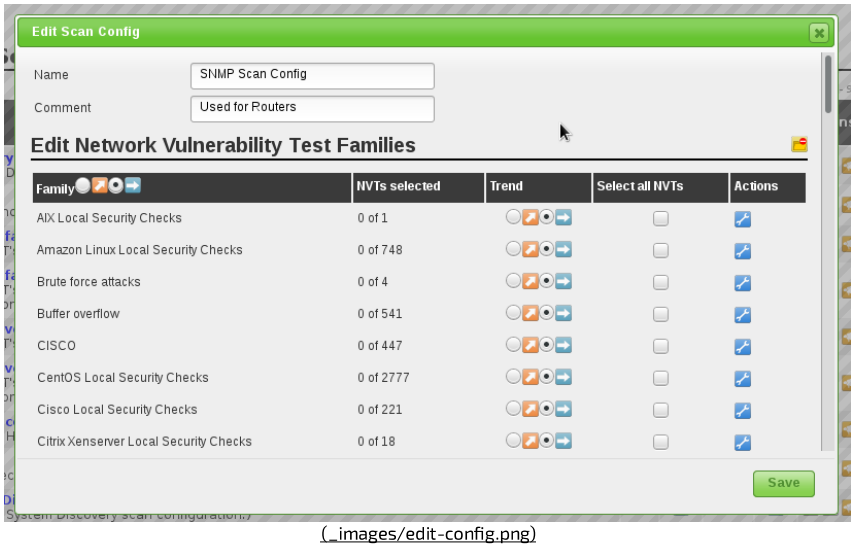
A new scan configuration can be created manually.

When manually creating a scan configuration enter the name and an optional comment and decide which scan configuration to use as a template. You can choose between:

- Empty, static and fast
- Full and fast

If another scan configuration should be used as a template it may be cloned on the overview page (_images/clone.png). After cloning the configuration can be edited and given its own name and comment and can be further customized.

The next overlay will display the starting configuration. The configuration can be edited right away.



(_images/edit-config.png)

The configuration offers many customization options.

Of importance are the following settings:

Family Trend

This option decides whether a newly introduced family will be activated in this scan configuration.

(_images/family-trend.png)

NVT Trend

In every family it can be decided if all NVTs in this family should be activated automatically.

(_images/nvt-trend.png)

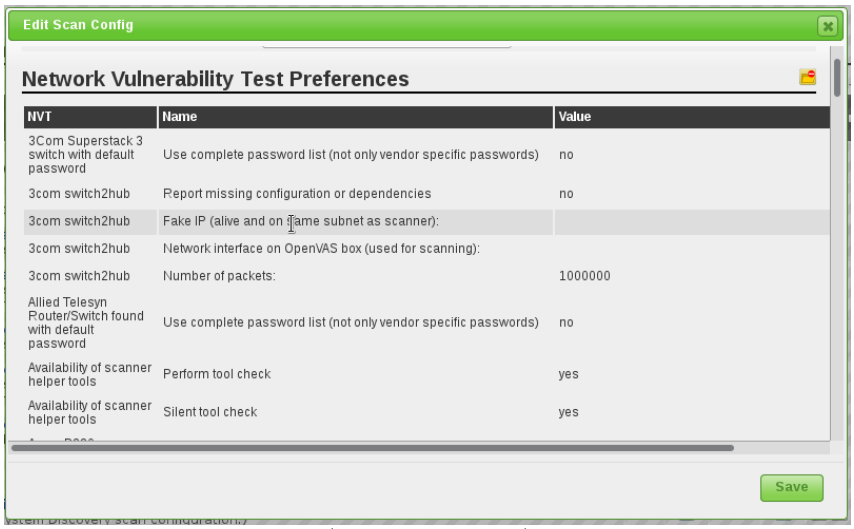
Select all NVTs

In this column all NVTs of a family may be selected.

Action (_images/edit.png)

With this icon the NVTs within a family may be individually selected if you do not want to use all of them.

When scrolling further down the *Edit Scanner Preferences* will appear (see section Scanner Preferences). Here additional settings for the scan can be customized after unfolding using (_images/fold.png). Also, there are the *Network Vulnerability Test Preferences* that are being used by the NVTs. They can be customized here after unfolding using (_images/fold.png). Furthermore, there is the possibility to define the settings directly within the respective NVTs.

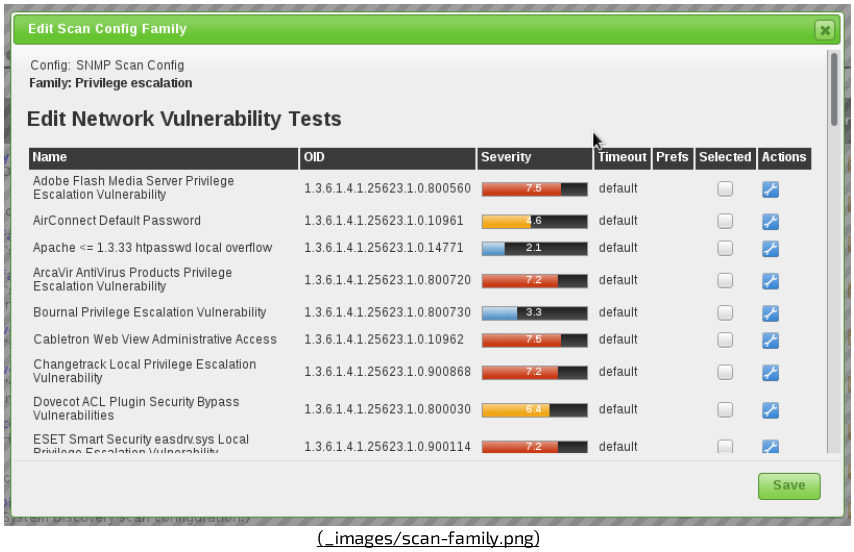


(_images/nvt-prefs.png)

The configuration allows for specific customization of the NVTs as well.

To make changes to the NVTs you must switch into the respective family.

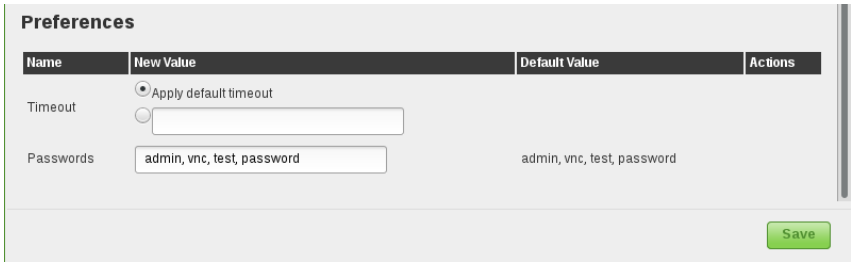
After selecting a family, the individual NVTs can be accessed. The NVTs that are part of a family and their severity can be viewed.



(_images/scan-family.png)

When accessing a family, the individual NVTs can be seen.

Also, the status (enabled/disabled) and the timeout of the NVT plugin can be viewed and verified as well if the NVT can be configured further via a configuration (column Prefs). If this is the case, the configuration can be accessed via the respective wrench icon (_images/edit.png). The settings can be found all the way at the bottom of the page the opens next.



(_images/nvt-pref.png)

The preferences can be configured for each NVT individually.

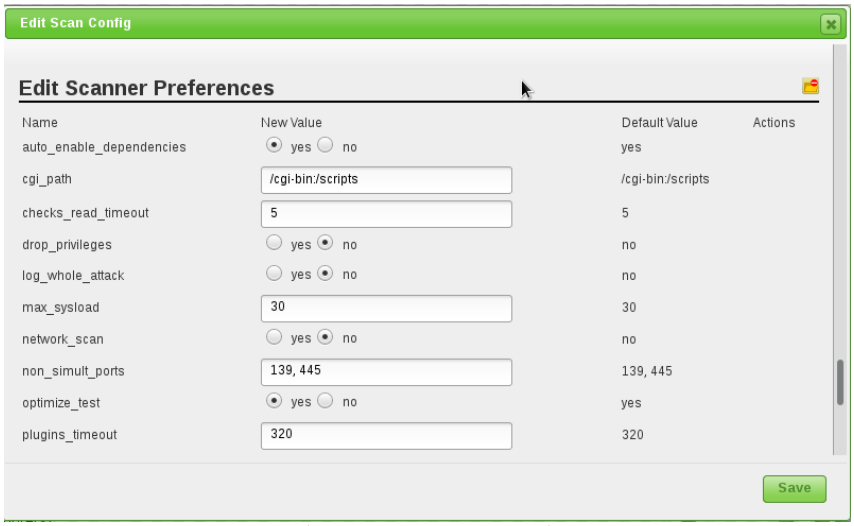
The customized settings of the NVTs are then visible on the overview page of the scan configuration (see figure The configuration offers many customization options. and The configuration allows for specific customization of the NVTs as well.).

For practical use especially the settings of the Port Scanner in use are of interest. The GSM appliance utilizes Nmap and Ping as port scanner. Nmap is being used via the NASL wrapper. This allows for the greatest flexibility.

9.2.2. Scanner Preferences

To document all scanner and NVT preferences is out of scope of this document. Therefore, only the most important general settings and specific settings of the Ping and Nmap-scanners will be covered.

9.2.2.1. General Preferences



(_images/scanner-prefs2.png)

These settings will be used in general by the configuration.

- *auto_enable_dependencies*: NVTs that are required by other NVTs will be activated automatically.
- *cgi_path*: This is the path that will be used by the NVTs to access CGI scripts.
- *checks_read_timeout*: This is the timeout for the network sockets during a scan.
- *drop_privileges*: With this parameter the OpenVAS scanner gives up *root* privileges before the start of the NVTs. This increases the security but results in fewer findings with some NVTs.
- *max_sysload*: This option specifies the maximum load on the GSM. Once this load is reached, no further NVTs are started until the load drops below this value again.
- *min_free_mem*: This option specifies the minimum available memory (in MB) which should be kept free on the GSM. Once this limit is reached, no further NVTs are started until sufficient memory is available again.
- *network_scan*: Experimental option, which scans the entire network all at once instead of starting Nmap for each individual host. This can save time in specific environments.
- *non_simult_ports*: These ports are not being tested simultaneously by NVTs.
- *optimize_test*: NVTs will only be started if specific pre-requisites are met (i.e. open port or detected application).
- *plugins_timeout*: Maximum run time of a NVT.
- *report_host_details*: Detailed information of the host are being saved to the report.
- *safe_checks*: Some NVTs can cause damage on the host system. This setting disables those respective NVTs.
- *scanner_plugins_timeout*: This is the maximum lifetime (in seconds) for all NVTs from the Port scanners family. If a NVT runs longer, the plugin is terminated.
- *time_between_request*: This option allows to set a wait time (in milliseconds) between two actions like opening a TCP socket, sending a request trought the open tcp socket, and closing the TCP socket.
- *timeout_retry*: number of retries when a socket connection attempt times out.
- *unscanned_closed*: This parameter defines if TCP ports that were not scanned should be treated like closed ports.
- *unscanned_closed_udp*: This parameter defines if UDP ports that were not scanned should be treated as closed ports.
- *use_mac_addr*: Systems will be identified by MAC address and not by IP address. This could be beneficial in a DHCP environment.
- *vhosts*: If the GSM is to scan a web server with name based virtual hosts then the settings *vhosts* and *vhosts_ip* can be used. In the setting *vhosts* the names of the virtual hosts an entered comma separated.
- *vhosts_ip*: If the GSM is to scan a web server with name based virtual hosts then the settings *vhosts* and *vhosts_ip* can be used. In the setting *vhosts_ip* the IP address of the web server is being entered. In the report it can not be referenced in which virtual instance a NVT discovered a vulnerability.

9.2.2.2. Ping Preferences

The Ping-Scanner-NVT from the Port Scanners family contains the following configurations parameters.

Remember that the `Alive Test` settings of a target object can overwrite some settings of the Ping-Scanner.

- *Do a TCP ping*: Here it can be selected if the reachability of a host should be tested using TCP. In this case the following ports will be tested: 21,22,23,25,53,80,135,137,139,143,443,445. Default: No.
- *Do an ICMP ping*: Here it can be selected if the reachability of host should be tested using ICMP. Default: Yes.
- *Mark unreachable Hosts as dead*: Here it can be selected if a system that are not discovered by this NVT should be tested by other NVTs later. Default: No.
- *Report about reachable Hosts*: Here it can be selected if the systems discovered by this NVT should be listed. Default: No.
- *Report about unreachable Hosts*: Here it can be selected if the systems that are not discovered by this system should be listed. Default: No.
- *TCP ping tries also TCP-SYN ping*: The TCP ping uses by default a TCP-ACK packet. Here a TCP-SYN packet can be used additionally. Default: No.
- *Use ARP*: Here it can be selected if hosts should be searched for in the local network using the ARP protocol. Default: No.
- *Use Nmap*: Here it can be selected if the Ping-NVT should use Nmap. Default: Yes.
- *nmap: try also with only –sP*: If Nmap is used the Ping-Scan will be performed using the –sP option.
- *nmap additional ports for –PA*: Here additional ports for the TCP-Ping-Test can be specified. This is only the case if *Do a TCP ping* is selected. Default: 137,587,3128,8080.

9.2.2.3. Nmap NASL Preferences

The following options from the Nmap (NASL Wrapper) NVT from the family of Port Scanners will be directly translated into options for the execution of the nmap command. Therefore, additional information can be found in the documentation for nmap (https://nmap.org/docs.html).

- *Do not randomize the order in which ports are scanned*: Nmap will scan the ports in ascending order.
- *Do not scan targets not in the file*: Only meaningful in conjunction with *File containing grepable results*.
- *Fragment IP packets*: Nmap fragments the packets for the attack. This allows bypassing simple packet filters.
- *Identify the remote OS*: Nmap tried to identify the operating system.
- *RPC port scan*: Nmap tests the system for Sun RPC ports.
- *Run dangerous ports even if safe checks are set*: UDP and RPC scans can cause problems and usually are disabled with the setting *safe_checks*.
- *Service scan*: Nmap will try to identify services.
- *Use hidden option to identify the remote OS*: Nmap will try to identify more aggressively.
- *Data length*: Nmap adds random data of specified length to the packet.
- *Host Timeout*: Defines the host timeout.
- *Initial RTT timeout*: This is the initial round trip timeout. Nmap can adjust this timeout dependent on the results.
- *Max RTT timeout*: This is the maximum RTT.
- *Min RTT timeout*: This is the minimum RTT.
- *Max Retries*: Maximum number of retries.
- *Maximum wait between probes*: This regulates the speed of the scan.
- *Min RTT Timeout*: This regulates the speed of the scan.
- *Minimum wait between probes*: This regulates the speed of the scan.
- *Ports scanned in parallel (max)*: Defines how many ports should be scanned simultaneously.
- *Ports scanned in parallel (min)*: see above
- *Source port*: Defines the source port. This is of interest when scanning through a firewall if connections are in general allowed from a specific port.
- *File containing grepable results*: Allows for the specification of a file in which line entries in the form of `Host: IP address` can be found. If the option *Do not scan targets not in the file* is set at the same time only systems contained in the file will be scanned.
- *TCP scanning technique*: Define the actual scan technique.
- *Timing policy*: Instead of changing the timing values individually the timing policy can be modified.

The timing policy uses the following values:

	initial_rtt_timeout	min_rtt_timeout	max_rtt_timeout	max_parallelism	scan_delay	max_scan_delay
Paranoid	5 min	100 ms	10 sec	Serial	5 min	1 sec
Sneaky	15 sec	100 ms	10 sec	Serial	15 sec	1 sec
Polite	1 sec	100 ms	10 sec	Serial	400 ms	1 sec
Normal	1 sec	100 ms	10 sec	Parallel	0 sec	1 sec
Aggressive	500 ms	100 ms	1250 ms	Parallel	0 sec	10 ms
Insane	250 ms	50 ms	300 ms	Parallel	0 sec	5 ms

9.3. Obstacles while Scanning

This section will highlight and explain several typical problems which might occur during a scan using the default values of the GSM. While the default values of the GSM are valid for most environments and customers, depending on the actual environment and the configuration of the scanned hosts they might require some tweaking.

The following sections will cover typical problems, explain why they occur and will give some advice to overcome these problems.

9.3.1. Hosts not found

During a typical Scan (either a Discovery Scan or a Full and Fast Scan) the GSM will by default first use the ping command to check the availability of the configured targets. If the target does not reply the ping request the target is presumed to be dead and will not be scanned by the port scanner or any NVT.

In most LAN environments this does not pose any problems because all devices will respond to a ping request. But sometimes (local) firewalls or other configuration might suppress the ping response. If this happens the target will not be scanned and will not be included in the results and the scan report.

To remediate this problem, both the target configuration and the scan configuration support the setting of the Alive Test (see Alive Test).

If the target does not respond to a ping request, you may want to test a `TCP Ping` . If the target is located within the same broadcast domain, you may want to try a `ARP Ping` as well.

9.3.2. Long Scanperiods

Once the target is discovered to be alive using the ping command the GSM uses a port scanner to scan the target. By default, a TCP port list containing around 5000 ports is used. If the target is protected by a (local) firewall dropping most of these packets the port scan will need to wait for the timeout of each individual port. If your hosts are protected by (local) firewalls you may want to tune the port lists or your firewalls. If the firewall does not drop the request but rejects the request the port scanner does not have to wait for the timeout. This is especially true if you include UDP ports in the scan.

9.3.3. NVT not used

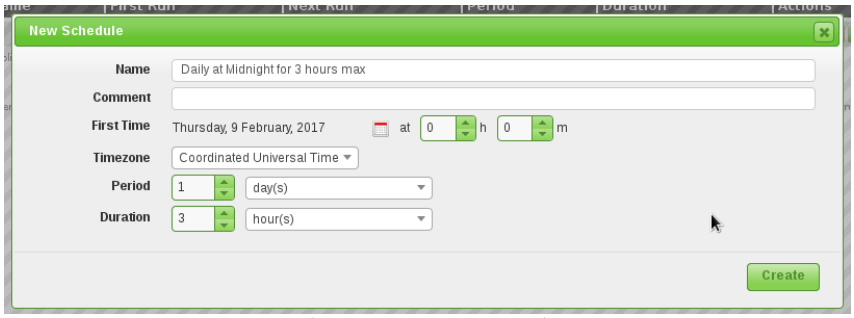
This happens especially very often if you use UDP based NVTs like NVTs using the SNMP protocol. If you use the default configuration `Full and Fast` , the SNMP NVTs are included. But if the target is configured using the default port list, the NVTs are not executed. This happens because the default port list does not include any UDP ports. Therefore, the port 161/udp (snmp) is not discovered and excluded from further scans. Both the discovery scans and the recommended `Full and Fast` scan configuration optimize the scan based on the discovered services. If the UDP port is not discovered, no SNMP NVTs are executed.

Please do not enable all ports per default in your port lists. This will prolong the scans considerably. Best practice is the tuning of the port lists to the ports which are used in your environment and are supported by your firewalls.

9.4. Scheduled Scan

For continuous vulnerability management the manual execution of task is cumbersome. The GSM supports the scheduling of tasks for their automation. This is done via *Schedules*. This option can be found in the *Configuration* menu.

The GSM does not provide any schedules by default. To add a new schedule use the|new| button in the upper left corner.



(_images/new-schedule.png)

Schedules support time controlled scans.

The Greenbone Security Manager refers to Schedules as automatic scans at a specific time. They can be run once or repeatedly. The intervals can be configured:

- hourly
- daily
- weekly

- monthly

Since the GSM runs in the UTC timezone internally, the time zone chosen in the schedule is very important. A drop down menu provides the available timezones. For Eastern Standard Time (EST) you will likely choose `America/New York` . Finally, the maximum duration of the scan can be limited. If the scan takes longer, it will be suspended until the next scheduled time slot becomes available.

This way it can be ensured that the scan will always run with a specific (maintenance) time window.

The following options are configurable in the dialog:

- **Name**
  This is a descriptive name. Meaningful are entries such as `Daily 5:15pm` or `Every 2nd monthly 4:15am` .

- **Comment**
  Enter a comment again.

- **First Time**
  Enter the time of the first run.

- **Timezone**
  The timezone the time refers to. UTC is default.

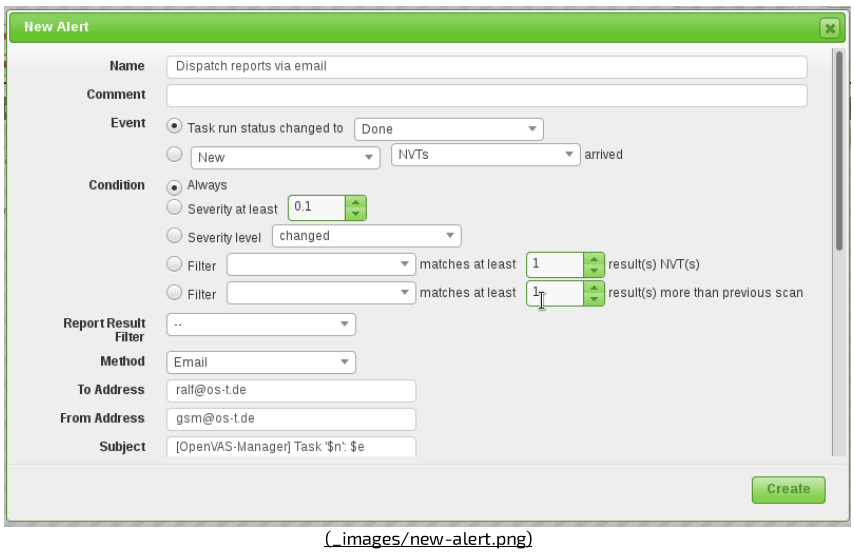
- **Period**
  This is the interval between two runs. It can be selected between hourly, daily, weekly and monthly. If left blank, the interval is a single instance.

- **Duration**
  This is the maximum duration a task can take for its execution. After expiration of the time allotted, the task is aborted.

9.5. Alerts

With the use of alerts the state and results of a scan can be sent to other systems automatically. Alerts are anchored within the system in a way that each configured event will trigger an action, for example, when a task is started or completed. Additionally, this can be tied to a condition. Such a condition could be the discovery of a vulnerability with a severity greater than 9. If met, an email or a SNMP trap can be triggered.

To create a new alert change to *Configuration/Alerts*. Now add a new alert using the button (_images/new.png) in the upper left corner.



(_images/new-alert.png)

Alerts offer various alerting options.

Using the overlay the following details of the alert can be defined:

Name:

The name, describing the alert, can be freely chosen

Comment:

The optional comment can contain additional information.

Event:

Here the event, for which the alert message is being sent, is being defined. For example, this can occur when the status of a task changes.

Condition:

Here additional conditions, that have to be met, may be defined. The alert message can occur:

- Always
- Only when at minimum a specific severity level is reached.
- If the severity level changes, increases or decreases.
- If a powerfilter matches at least the specified number of results.
- If a powerfilter matches at least the specified number of results more than in the previous scan.

Report Result Filter

Finally the results can be limited with an additional filter. A filter must be created and saved prior (see section Powerfilter (gui_introduction.html#powerfilter)).

Method:

Here the method for the alert is selected. Only one method per alert can be chosen. If different alerts for the same event should be triggered, multiple alerts must be created and linked to the same task.

Email

This is the most powerful and most used method. To use this method the mailserver to be used must be configured using the GSM console (see section Mail Server (systemadministration.html#mail-server)). The following options may be specified:

To Address:

This is the email address to which the email should be sent to.

From Address:

This is the sender address of the generated email.

Subject:

This is the subject of the email. You can use variables like $n (task name) and $e (event description).

Content:

Here the content of the email can be defined:

Simple Notice:

This is only a simple description of the event.

Include Report:

If the event for the completion of the task (Default: Done) is selected the report can be included in the email. Here a report format that uses the content type *text/** can be chosen as an email does not support binary content directly. Additionally, you can modify the contents of the email message. Within the message you may use variables:

- $c condition description
- $e event description
- $F name of filter
- $f filter term
- $H host summary
- $i report text
- $n task name
- $r report format name
- $t a note if the report was truncated
- $z timezone

Attach Report:

If the event for the completion of the task (Default: Done) is selected the report can be attached to the email. Here any report format can be chosen. The report will be attached in its correct MIME type to the generated email. PDF is possible as well. Additionally, you can modify the contents of the email message. The same variables may be used.

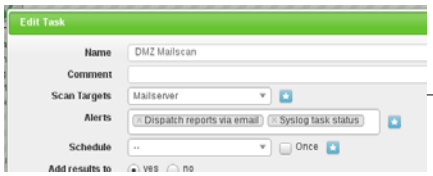
System Logger

This method sends the alert to a Syslog daemon. The Syslog server is defined via the console (see section Central Logging Server (systemadministration.html#central-logging)).

HTTP Get

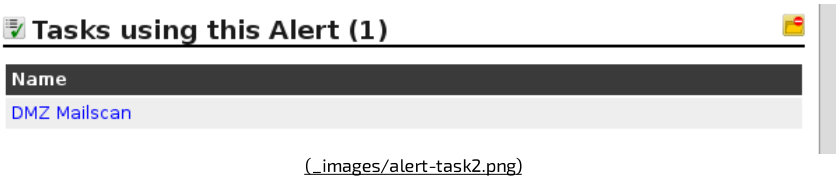
With the HTTP Get method, an SMS text message or a message to a trouble ticket system can be sent automatically, for example. The following variables can be used when specifying the URL:

- `$n` : Name of the task
- `$e` : Description of the event (Start, Stop, Done)
- `$c` : Description of the condition that occurred
- `$$` : The $ symbol



(_images/alert-task.png)

Tasks need to be configured with the appropriate alerts.



(_images/alert-task2.png)

In an alert is in use the corresponding tasks are referenced.

Sourcefire Connector

Here the data can be sent automatically to a Cisco Firepower Management Center (formerly known as Sourcefire Defense Center). For more information see section Firepower Management Center (connecting.html#sourcefire).

verinice.PRO Connector

Here the data can be sent automatically to a verinice.PRO installation. For more information see section Verinice (connecting.html#verinice).

Send to Host

Here the report may be sent via TCP to an arbitrary host/port combination. The format of the report may be chosen from the installed report formats.

SCP

The report may be copied to a host via scp. Within the filename you can use the following variables:

- $$: $
- $n: task name

Additionally, the remote host and the credentials for login must be specified. The Known Hosts field provides the public key of the remote host.

SMB

The report may be copied to a host via SMB. Within the filename you can use the following variables:

- $$: $
- $n: task name

Additionally, the remote host, the share name and the credentials for login must be specified. Since the SMB protocol does not offer fingerprints to establish mutual trust, man-in-the-middle attacks cannot be fully prevented.

SNMP

An SNMP trap is sent to the given agent. Within the message you can use the following variables:

- $$: $
- $e: event description
- $n: task name

The provided community is used to authenticate the SNMP trap and the agent ist the targeted SNMP trap receiver.

Start Task

Here the alert may start an additional task. The available tasks are selected using a drop down menu.

For the alert to be used afterwards, a specific task definition must be created (see figure Tasks need to be configured with the appropriate alerts.). To do so edit the respective task. This change of the task is also allowed for already defined and used tasks as it does not have any effect on already created reports.

Afterwards the respective alert references the tasks using the alert (see figure In an alert is in use the corresponding tasks are referenced.).

9.6. Reports and Vulnerability Management

The results of a scan are summarized in a report. Reports can be viewed with a browser and

downloaded from the GSM in different formats. Once a scan has been started, the report of the results found so far can be viewed. Once a scan is complete, its status changes to `Done` . From now on no additional results will get added. For more information on reports please refer to the *Reports* (reports.html) chapter as well.

(_images/reportsummary.png)

The report summary gives an overview over vulnerabilities found.

The report summary gives a quick overview over the current state. It shows if a scan is complete and how many vulnerabilities have already been found. From the summary a report can be downloaded directly in different formats. The following formats are supported (see also section Report Plugins (reports.html#report-plugins))

Anonymous XML

Like XML but anonymous.

ARF: Asset Reporting Format v1.0.0

This format creates a report that represents the NIST Asset Reporting Format.

CPE - Common Enumeration CSV Table

This report selects all CPE tables and creates a single comma separated file.

CSV hosts

This report creates a comma separated file containing the systems discovered.

CSV Results

This report creates a comma separated file with the results of a scan.

GSR PDF - Greenbone Security Report (recommended)

This is the complete Greenbone Security report with all vulnerabilities.

GXR PDF - Greenbone Executive Report (recommended)

This is a shortened report for management.

HTML

This report is in HTML format.

ITG - IT-Grundschutz catalogue

This report is guided by the BSI IT-Grundschutz catalogue.

LaTeX

This report is offered as LaTeX source text.

NBE

This is the old OpenVAS/Nessus report format.

Verinice ISM, ITG

For Import into veri.nice.

XML

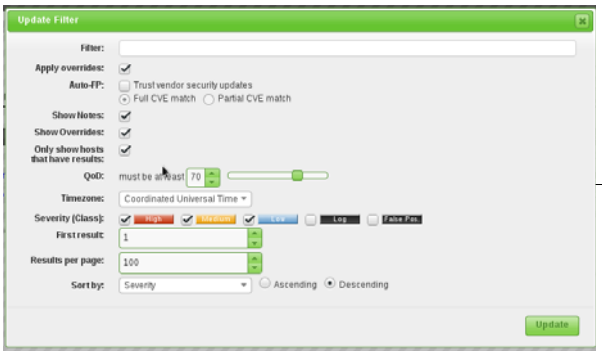
A single XML file is created from the report details. This should be the basis for creating your own style for a report or post-process the results in other ways.

Details of a report can be viewed in the web UI as well.

(_images/report-darstellung.png)

Different views of the same report.

Since a report often contains a lot of findings, the complete report as well as only filtered results can be viewed and downloaded. In the default setting only the `High` and `Medium` risks are being displayed. This can be changed very easily.



(_images/reportfilter.png)

Report Filtering.

In the Filtered Results section shows the filtered results. As long as the scan is still running, changes can cause rearrangements here.

To interpret the results please note the following information:

- False Positives False Pos. (_images/false_positive.png)

  A false positive is a finding that describes a problem that does not exist in reality. Vulnerability scanners often find evidence that point at a vulnerability. However, a final judgment cannot be made. There are two options available:

  - Reporting of a potentially nonexistent vulnerability (False Positive).
  - Ignoring reporting of a potentially existing vulnerability (False Negative).

  Since a user can identify, manage and as such deal with false positives compared to false negatives, the GSM Vulnerability Scanner reports all potentially existing vulnerabilities. The GSM assists with several automatic and semi-automatic to categorize them.

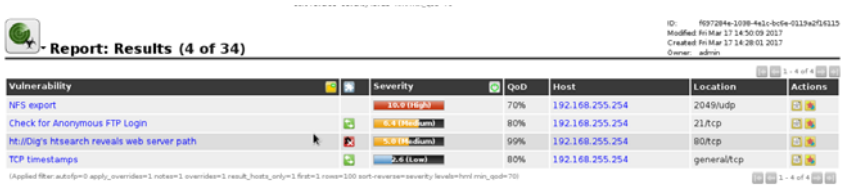
  This problem is very common with Enterprise Linux distributions. If, for example, an SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If the user knows of this circumstance an Override can be configured (see section Overrides and False Positives). The AutoFP function (see section Automatic False Positives) can assist here as well.

> **Note**
>
> Consider the new concept of Quality of Detection (see sections Reading of the Reports and Network Vulnerability Tests).

- Multiple findings can have the same cause. If an especially old software package is installed, often multiple vulnerabilities exist. Each of these vulnerabilities is tested by an individual NVT and causes an alert. The installation of a current package will then remove a lot of vulnerabilities at once.
- Important are findings of the levels High High (_images/high.png) and Medium Medium (_images/medium.png). Address these findings in order of priority. Before addressing medium level findings, high level findings should get addressed. Only in exceptional cases, when it is known that the high alerts need to be less considered (because the service cannot be reached through the firewall) should this approach be deviated from.
- Low Low (_images/low.png) and Log Log (_images/log.png) are mostly interesting for detail understanding. This is why these findings are filtered out by default. These findings can hold very interesting information however and considering them will increase the security of your network and systems. For their understanding often a deeper knowledge of the applications is required. Typical for an alert at the log level is that a service uses a banner with its name and version number. This could be useful for an attacker during an attack if this version has a known vulnerability.
- To simplify the remediation of vulnerabilities every alert offers a solution for problems directly. In most cases it will be referred to the latest vendor software package. In some cases a configuration change will be mentioned.
- References explain the vulnerabilities further. Even though the alerts contain a lot of information, external references are always listed. These refer to web sites on which the vulnerability was already discussed. Additional background information is available such as who discovered the vulnerability, what effects it could have and how the vulnerability can be remediated.

9.6.1. Reading of the Reports

The report contains a list of all the vulnerabilities detected by the GSM (see figure List of discovered vulnerabilities)



(_images/reportvuln.png)

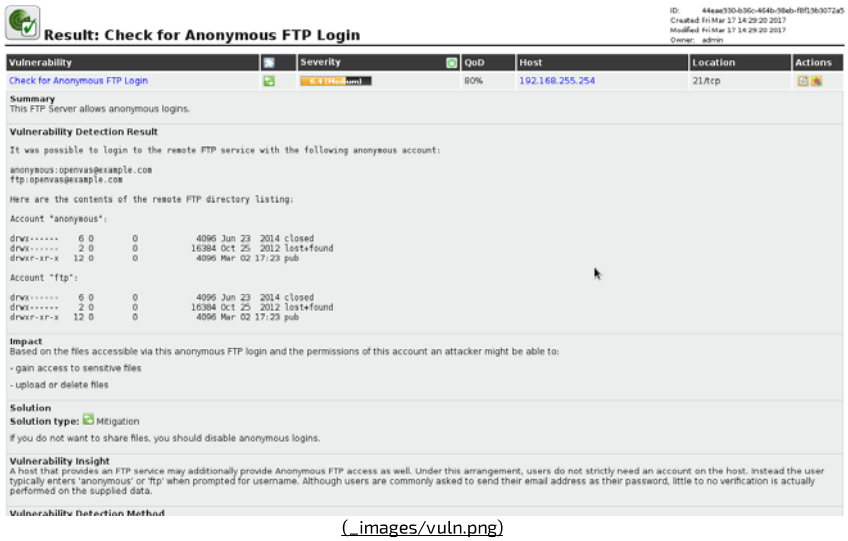
List of discovered vulnerabilities

To support the administrator with the analysis of the results the severity of a vulnerability (CVSS, see also section CVSS)is displayed directly as a bar.

To point the administrator to a simple solution the column Solution-Type (_images/solution_type.png) displays the existence of a solution. The column will display if a vendor patch (_images/st_vendorfix.png) exists or a workaround (_images/st_workaround.png) is available. It will also be displayed if no solution for a vulnerability exists (_images/st_nonavailable.png). If the column of the respective vulnerability still appears empty then the respective NVT has not been updated yet.

The column Quality of Detection (QoD) provides information in regard to the reliability of the successful detection of a vulnerability. This assessment is implemented into all existing NVTs step by step (see section Network Vulnerability Tests). This column allows to be filtered as well. You can use the *min_qod* in the Powerfilter. By default, only NVTs with a QoD of 70% are displayed. Vulnerabilities with a lower reliability of detection are not displayed in the report. The possibility of false positives is thereby lower.

In the respective vulnerability view, additional, more detailed information is available.

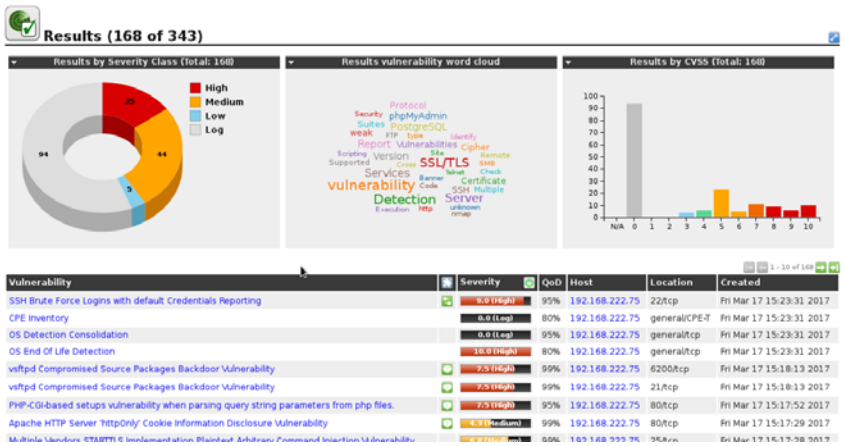


(_images/vuln.png)

Detailed information about the vulnerability and solution options.

9.6.2. Results

While the reports only contain the results of one single run of a task all results are saved in the internal database and can be viewed using *Scan Management/ Results*.



(_images/allresults.png)

By default, the view is sorted by the creation time of the results. But the results may be sorted by severity, QoD, solution type or host as well. Additionally, powerfilters (see section Powerfilter (gui_introduction.html#powerfilter)) may be used to view just the interesting results.

9.6.3. Notes

Notes allow adding comments to a Network Vulnerability Test (NVT). They will also be displayed in the reports. A Note can be added to a specific result, a specific task, a risk level, port or host and as such will only appear in specific reports. A Note can be generalized just as well so that it will be displayed in all reports.

9.6.3.1. Creating notes

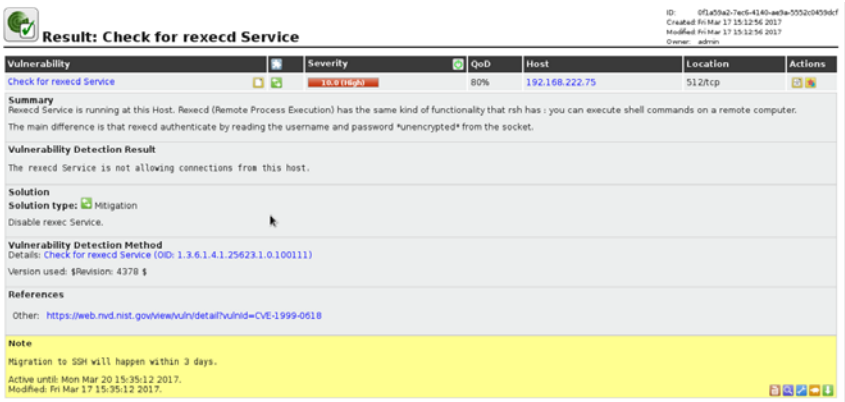
To create a new note select the finding in the report you want to add a note to and click *New Note* (_images/new.png). Alternatively you can create a note without relation to a finding. However, the GSM can not suggest any meaningful values for the different fields in the following dialogue.

A new window opens in which exactly those criteria of the selected vulnerability are pre-set.

(_images/newnote-edit.png)

A new note

Individual values can be selected and unselected to generalize or the note even further or make it more specific. Additionally, the note can be activated for a specific period of time. This allows adding of information to a note that a security update is uploaded in the next seven days. For the next seven days the note will be displayed in the report that the vulnerability is being worked on.

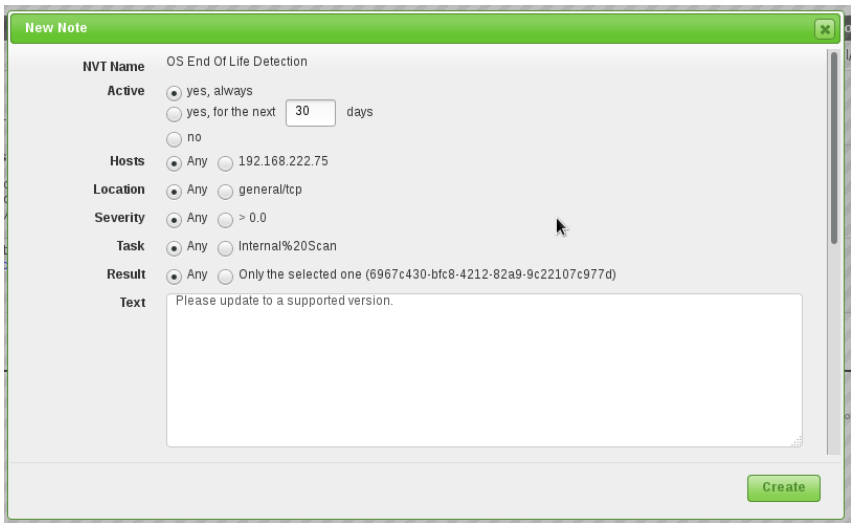


(_images/noteresult.png)

A note in a report

9.6.3.2. Generalizing Notes

Any note can be generalized. In this example a quite extensive generalization is configured, matching any target host, port and task.



(_images/note-generalize.png)

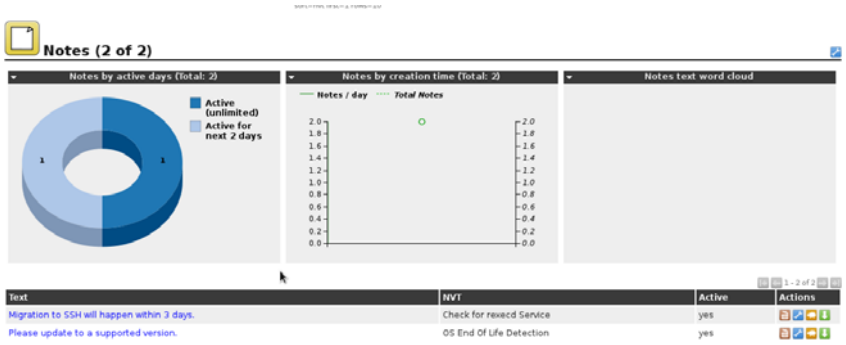
A generalized note

From this moment on the note is always shown in the results view if this NVT matches.

This applies for all previously created scan reports and for all future scan reports until the note is deleted.

9.6.3.3. Managing Notes

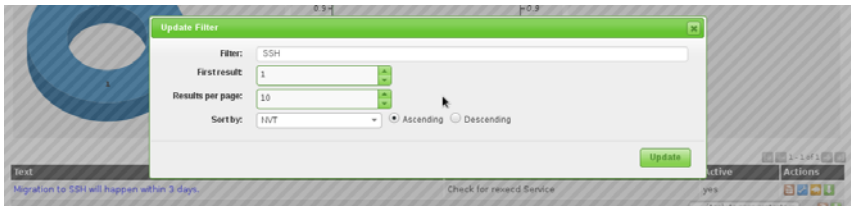
The created notes can be displayed under *Scan Management* and *Notes*. Here completely new notes can be added as well.



(_images/note-management.png)

Notes can be managed individually.

Among others, it is being displayed if created notes are currently active. Additionally, notes can be edited (_images/edit.png). To search for a specific note a search filter can be used respectively. This will make it easier to find a specific note, especially when many notes have been created. The search filter can be opened respectively end text entered appropriately or it can be entered directly into the filter window at the top. These filters can, of course, be saved for later use as well.



(_images/note-search.png)

Notes can be limited by a search filter.

9.6.4. Overrides and False Positives

The results of a report can not only be supplemented through meaningful or helpful data but the severity of the results can be modified. This is called Override by the GSM.

These overrides are especially useful to manage results that are discovered as a false positive and that have been given a critical severity but should be given a different severity (i.e. False Positive) in the future. The same is true for results that only have been given the severity Log but should be assigned a

higher severity locally. These can be managed with an override as well.

The use of overrides makes also sense to manage acceptable risks. The risk of a vulnerability can be ranked new and as such the risks that, in your opinion, are not critical can be re-evaluated in the results.

9.6.4.1. What is a false positive?

A false positive is a result that describes a problem that does not exist in reality. Often vulnerability scanners find proof that point to a security issue. A final prediction is not possible, however. Two options are now available:

- Reporting of a potentially non-existent vulnerability (False Positive).
- Omission of the reporting of the potentially existing vulnerability (False Negative).

Since a user is able to recognize, manage and handle these as it is not the case with false negatives, the GSM vulnerability scanner reports all potentially existing vulnerabilities. The GSM assists with several automatic and semi-automatic to categorize them.

> **Note**
>
> Consider the new concept of Quality of Detection (see sections Reading of the Reports and Network Vulnerability Tests).

This problem is especially typical with Enterprise Linux distributions. If, for example, an SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner which knows of a vulnerability in this version will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If the scan administrator knows of this circumstance, an override can ensure that these results are no longer being displayed.

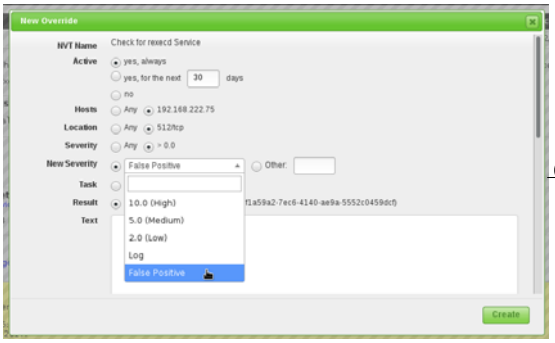
9.6.4.2. Creating an Override

Overrides like notes can be created in different ways. The simplest way to get to this option is through the respective scan result in a report. At the top right of each finding the *Add Override* icon (_images/new_override.png) can be found.

Overrides have the same function as notes, however, they add the possibility to adjust the severity:

- High
- Medium
- Low
- Log
- False Positive

Vulnerabilities with the level False Positive are not being displayed in the reports. But special reports for findings of this level can be created. As with overrides, they can have a time limitation.



(_images/overridenew.png)

Overrides allow for the customization of the severity level.

> **Note**
>
> If several overrides apply to the same NVT in the same report the most recent override is actually used and applied.

9.6.4.3. Disabling and Enabling Overrides

Wherever overrides may change the display of the results, the overrides may be enabled or disabled. This may be done using the icon (_images/overrides_enabled.png) in the title bar.

(_images/enable-overrides.png)

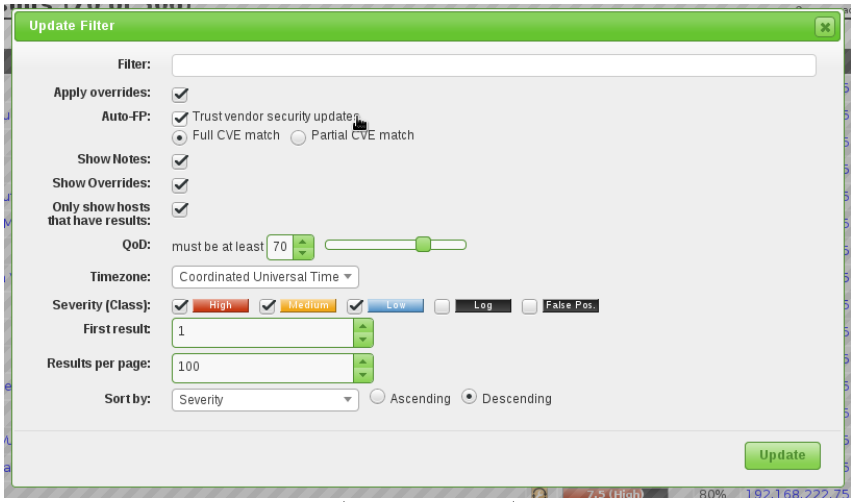
Overrides may be enabled and disabled.

9.6.4.4. Automatic False Positives

The GSM is able to detect false positives automatically and can assign an override automatically. However, the target system must be analyzed internally and externally with an authenticated scan.

An authenticated scan can identify vulnerabilities in locally installed software. As such vulnerabilities can be identified that can be exploited by local users or are available to an attacker if he already gained local access as an unprivileged user for example. In many cases an attack occurs in different phases and an attacker exploits multiple vulnerabilities to increase his privileges.

An authenticated scan offers a second more powerful function justifying its execution. In many cases by scanning the system externally, it can not be properly identified if a vulnerability really exists. In doubt, the Greenbone Security Manager reports all potential vulnerabilities. With the authenticated scan many of these potential vulnerabilities can be recognized and filtered as false positives.



(_images/autofp.png)

Automatic False Positives

This problem is especially typical with Enterprise Linux distributions. If, for example, an SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner which knows of a vulnerability in this version will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If an authenticated scan was performed the GSM can recognize that the version 4.4-p1 is installed and no longer contains this vulnerability.

Automatic false positives are enabled with the Report-Filter function (see section Powerfilter (gui_introduction.html#powerfilter)). This functionality gives the best results when using the `Partial CVE match` .

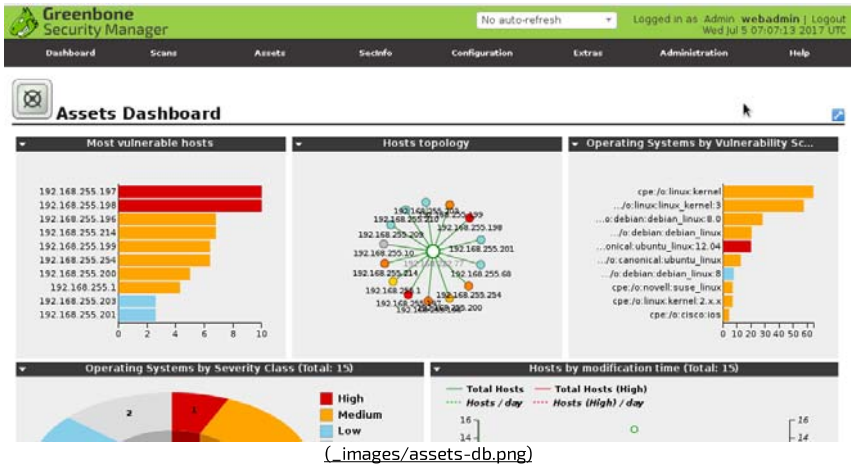
9.7. Asset Management

The GSM may store all results of all scans in the Asset-Management. When defining a task it can be determined if the results of a scan should be recorded in the asset management (see section Creating a Task).

While the asset management of older GOS versions is still available (see section Classic Asset Management) the new asset management offers additional features.

9.7.1. Dashboard

The dashboard provides a quick overview on the found and scanned systems including their operating systems, vulnerabilities and severities. The Dashboard may be accessed via *Assets* followed by *Dashboard*.

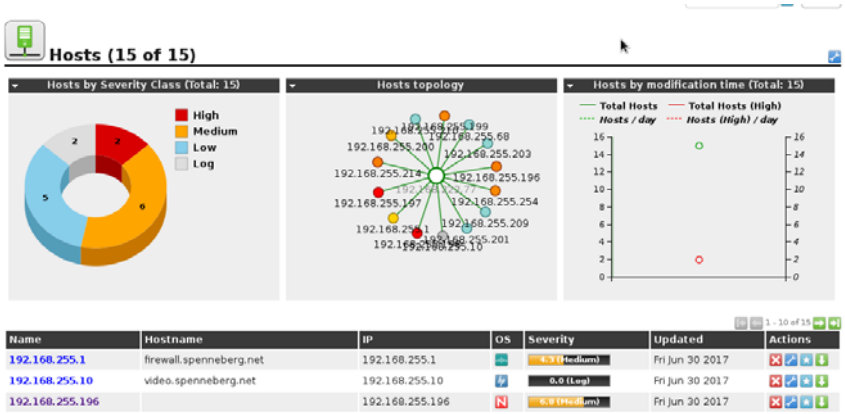


(_images/assets-db.png)

The asset dashboard provides a quick overview on the scanned systems.

9.7.2. Hosts View

The hosts view displays all scanned hosts individually.



(_images/assets-hosts.png)

The hosts view presents the hosts individually.

While displaying the main information on the hosts like IP addresses, hostname, operating system, and maximum severity this view may also be used to alter the stored information.

9.7.3. Modifying Hosts

The rightmost column contains four buttons allowing the following operations:

- (_images/delete.png) Delete the host from the asset management
- (_images/edit.png) Edit the host. Currently only comments may be added. Further options may be available in future releases.
- (_images/new.png) Create a scan target based on the asset. You will be redirected to the target creation and the hosts field will be prefilled.
- (_images/download.png) You may download the XML presentation of the asset.

The delete, create and download option are also available at the bottom of the page. These options apply then to all currently displayed hosts.

(_images/assets-hosts-bottom.png)

The hosts view support the creation of targets based on the displayed hosts.

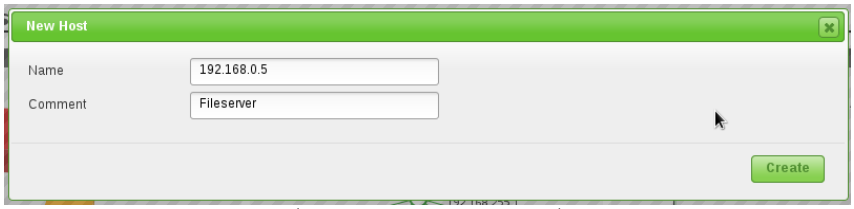
This may be used by first filtering the hosts. For example, you could create a filter to display only Microsoft Windows hosts. Then a new scan target could be defined based on the filtered hosts using the button (_images/new.png) at the bottom of the screen.

This will create a fixed set of hosts. If additional Microsoft Windows hosts show up in further scans they will not be added to the target!

9.7.4. Adding Hosts

If you want to add hosts to the asset management, this is possible as well. Currently you may only provide the IP address and a comment. Further options will be added in future GOS releases.

To add a host use the (_images/new.png) button at the left top of the page. An overlay is displayed supporting the entry of the IP address and a comment.



(_images/assets-hosts-add.png)

Adding hosts is possible using the WebUI.

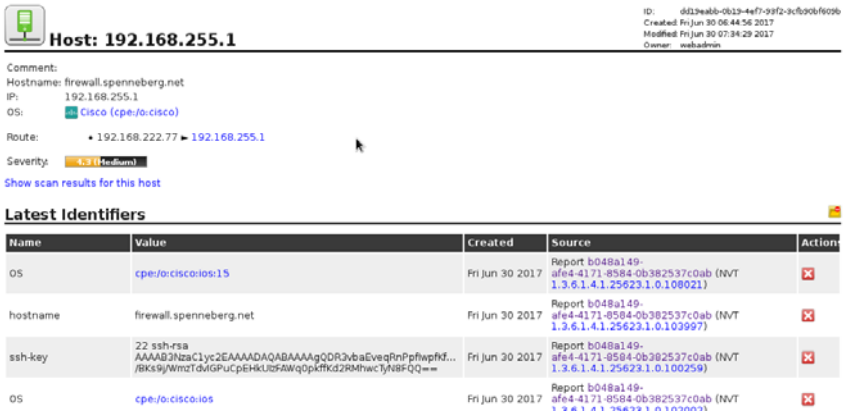
Of course this feature is also available via GMP (see section GMP (systemadministration.html#gmp)). The import of hosts from a configuration management database may be achieved using this option.

9.7.5. Host Details

When selecting a host, the host details are displayed. These include:

- Comment
- IP address
- Hostname
- Operating System
- Route
- Maximum Severity

Additionally, the identifiers of the system are displayed. Especially SSH keys and X.509 certificates will be presented.

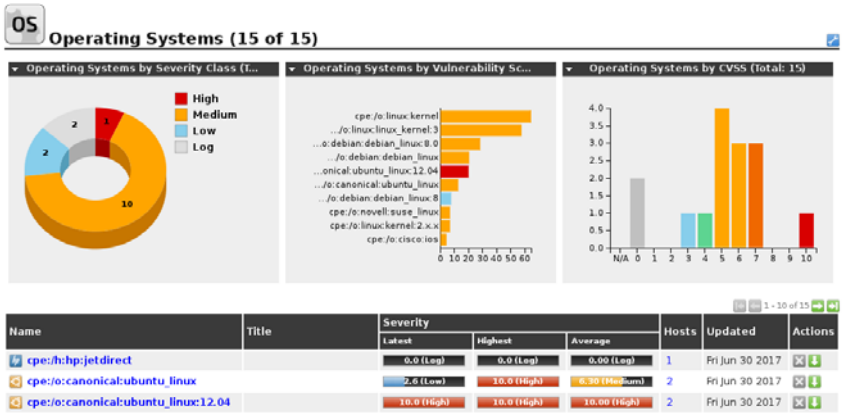


(_images/assets-hosts-details.png)

The hosts details present the identifiers of the host.

9.7.5.1. Operating Systems View

The operating systems view within the asset management provides a different view on the stored data. While the hosts view is centered on the individual hosts, this view concentrates on the used operating systems.

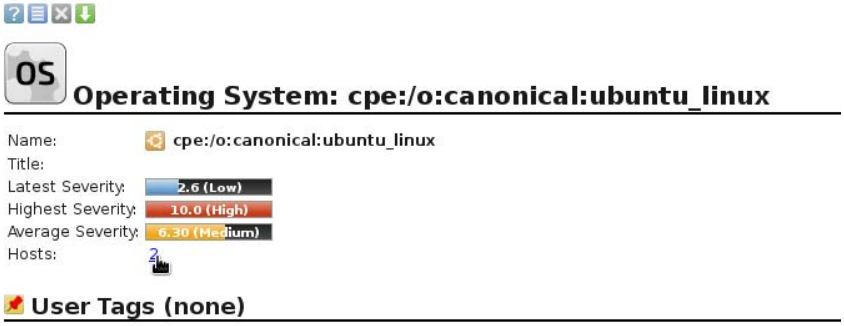


(_images/assets-os.png)

The OS view clusters the operating systems.

This view provides the average maximum severity of all hosts using the same OS and adds the latest and highest severity as well to the picture.

By selecting an operating system you can directly access the hosts using the OS.

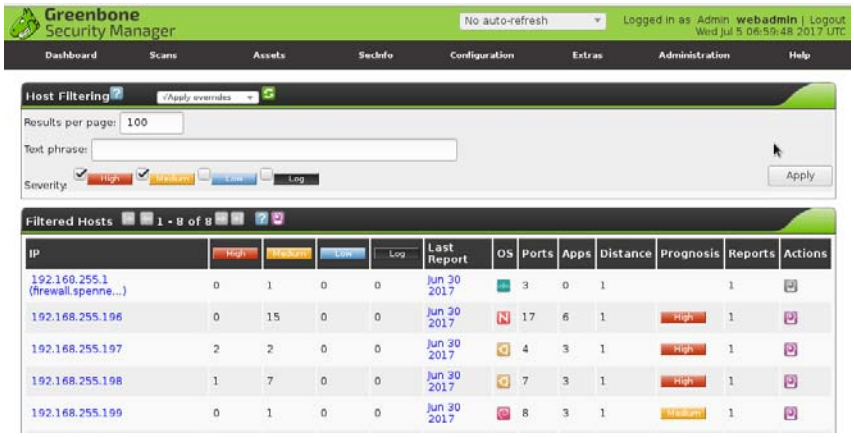


(_images/assets-os-details.png)

From the OS details the hosts using the OS may be displayed.

9.7.5.2. Classic Asset Management

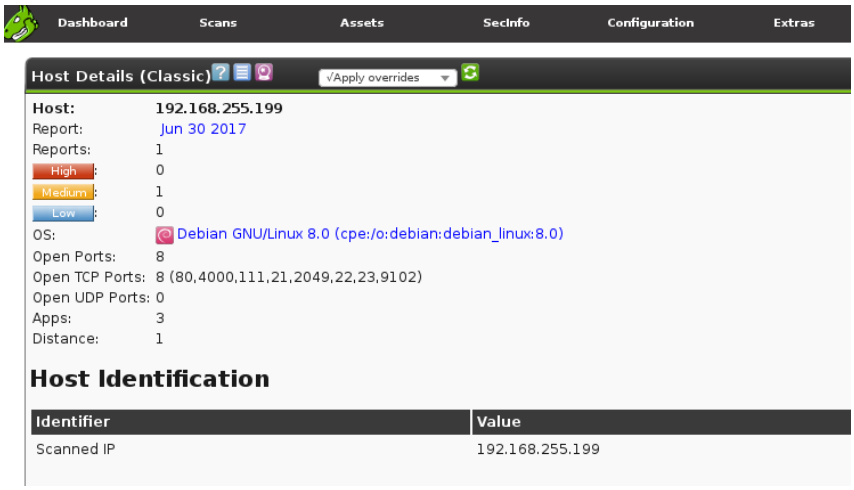
The classic asset management can be accessed via *Assets* followed by *Hosts (Classic)*.



(_images/assets-classic.png)

The asset database displays the stored systems.

Here you can see how many security holes were discovered on the systems. In addition, the overview displays the operating system with a logo (OS column) and the discovered ports and applications. Also, it is being displayed how a scan of the system would possible turn out at this moment (Prognosis column, see also section Prognosis). Via the (_images/prognosis.png) a prognostic report can be created as well. Through the asset management you can always access the last report of the host. The date of the report is visible and can be accessed directly by clicking on the link. If multiple reports exist, older reports can be accessed in the host details. By clicking on the host IP address the host details can be accessed. Here the amount of discovered vulnerabilities, the identified operating system, the discovered ports and the amount of detected applications on the system can be viewed



(_images/details-classic.png)

The host details contain further information on the host.

The host details contain additional information of the system:

Hardware:

The GSM stores information about the hardware. If the MAC address is known, it is listed here. It can only be displayed though if the target system is on the same LAN as the GSM.

Detected Applications:

Especially of interest are the detected applications. With this the Greenbone Security Manager can give a prognosis based on its SecInfo database without re-scanning if additional security risks would be found. This is especially of interest for systems that currently do not have any vulnerability and new scans are not being performed regularly.

9.7.6. Prognosis

The prognosis allows forecasting possible security risks without a new scan based on current information about known security holes from the *SecInfo Management* (SCAP, Security Content Automation Protocol) (see chapter SecInfo Management). This is especially interesting for environments where by the use of the GSM most vulnerabilities have been removed or remediated. Of course new vulnerabilities are being discovered daily. Not every vulnerability justifies a new scan of the network or of individual systems. Due to the fact that the GSM has this information, based on the knowledge of the detected applications it can make a prognosis which security risks exist. If security risks become known, it justifies the actual running of a scan to verify the prognosis. For this the asset database requires current data of course. This is why a scan of the systems should occur regularly in weekly or monthly intervals.

A prognostic scan can be performed as well. It will determine probable existing vulnerabilities

9.8. SecInfo Management

The *SecInfo Management* offers central access to different information relating to IT-Security. This includes the following information:

NVTs:

These are the Network Vulnerability Tests. These tests test the target system for potential vulnerabilities.

CVEs:

The Common Vulnerability and Exposures are vulnerabilities published by vendors and security researchers.

CPEs:

The Common Platform Enumeration offers standardized names of the products that are being used information technology.

OVAL Definition:

The Open Vulnerability Assessment Language offers a standardized language for the testing of vulnerabilities. OVAL definitions use this language to concretely discover vulnerabilities.

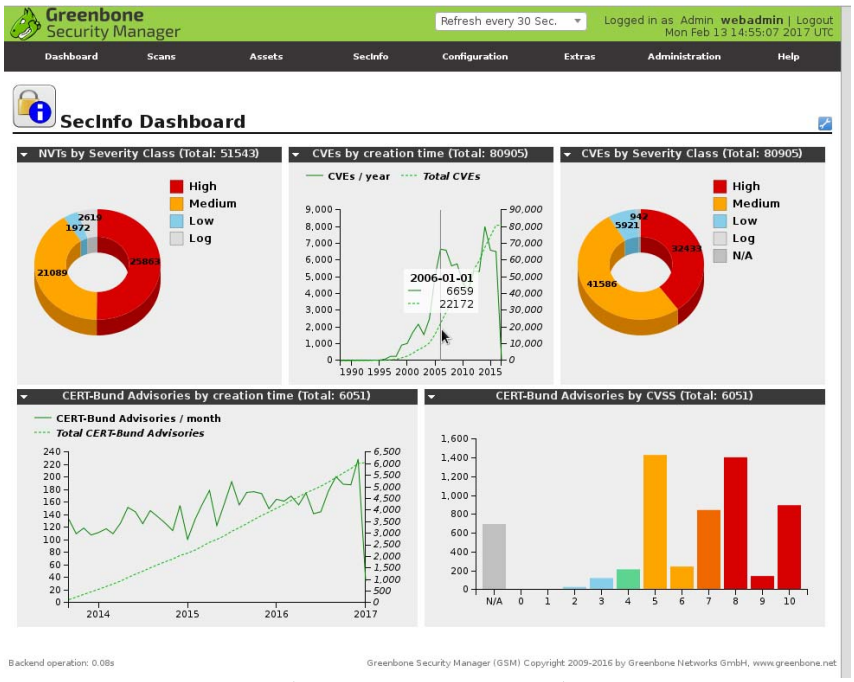
CERT-Bund Advisories:

The CERT-Bund Advisories are published by the emergency response team (https://www.cert-bund.de/) of the Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI). The main task of the CERT-Bund is the operation of a warning and information service publishing information regarding new vulnerabilities and security risks as well as threats for IT systems.

DFN-CERT Advisories:

The DFN-CERT (https://www.cert.dfn.de/) is the emergency response team of the German Research Network (German: Deutsches Forschungsnetz, abbreviated as DFN).

The CVEs, CPEs and OVAL definitions are published and made accessible by NIST as part of the National Vulnerability Database (NVD) (see also section Security Content Automation Protocol (SCAP)).



(_images/secinfo-dashboard.png)

The SecInfo Dashboard allows displaying data graphically.

To get a quick overview over this information the Secinfo dashboard (see figure The SecInfo Dashboard allows displaying data graphically.) exists. It allows for the graphical display of different information grouped by different aspects.

9.8.1. SecInfo Portal

SecInfo Data is being provided by Greenbone Networks online as well. This portal (https://secinfo.greenbone.net) can be accessed directly through the Internet. It corresponds to data that can be displayed in the GSM as well. The SecInfo Portal is a GSM ONE that has been configured especially for anonymous guest access. Contrary to a full-fledged GSM only the SecInfo management and the CVSS online calculator are available for the guest user.

The SecInfo portal achieves a multitude of functions:

- Anonymous access to details of the Greenbone vulnerability tests as well as SCAP data (CVE, CPE, OVAL) and messages of different CERTs. The data itself is referenced thus offering the possibility to browse by Security-Information regarding a product, a vendor or a specific vulnerability.
- Demo of the respective upcoming version of the Greenbone OS as soon as the SecInfo section reached beta status.
- Service for embedded diagrams as they are used on the Greenbone website for feed statistics for example.
- Service for direct links to details or specific selections, for example for a specific CVE (CVE-2014-0160, *Heartbleed*) or an overview: All published CVE notices in 2013.
- Service for links to CVSS vulnerability rating including CVSS online calculator: AV:N/AC:L/Au:N/C:P/I:P/A:P
- Example of how a GSM can be configured by yourself on an Intranet to allow direct links in internal reports and platforms.

Such access can be provided yourself by activating guest access (see section Guest Log in (gui_administration.html#guest-login))

9.8.2. Network Vulnerability Tests

The abbreviation NVT stands for Network Vulnerability Test. These are test routines the GSM utilizes and that are updated regularly with the Greenbone Security Feed. Here you can find information when the test was developed, which systems are affected, what impact the vulnerabilities have and how they can be remediated.

Compared to the Greenbone OS 3.0 there are two new pieces of information, the Solution Type (see Solution Type (glossary.html#glossary-solution-type)) and the Quality of Detection (QoD, see Quality of Detection (QoD) (glossary.html#glossary-qod)).

With the introduction of the QoD the parameter `Paranoid` in the scan configuration (see chapter Scan Configuration) is being removed without replacement. In the past a scan configuration without this parameter only used NVTs with a QoD of a minimum of 70%. Only with this parameter all NVTs were used. Now all NVTs are being used and executed in a scan configuration. The filtering of the results is done on based on QoD. That way all the results are always available in the database and can be turned on or off respectively.

9.8.3. Security Content Automation Protocol (SCAP)

The National Institute of Standards and Technology (NIST) in the USA provides the National Vulnerability Database (https://nvd.nist.gov/) (NVD). NVD is a data repository for the vulnerability management of the US government. The goal is the standardized provision of the data for the automated processing and support for the function of vulnerability management and the implementation of compliance guide lines. The NVD provide different databases. They include

- check lists
- vulnerabilities
- misconfigurations
- products
- threat metrics

For this the NVD utilizes the Security Content Automation Protocol (https://csrc.nist.gov/projects/security-content-automation-protocol/) (SCAP). The Security Content Automation Protocol is a combination of different interoperable standards. Many standards were developed or derived from public discussion. The public participation of the community in the development is an important aspect for accepting and spreading of the SCAP standards. The SCAP protocol is currently specified in version 1.2 and includes the following components:

- Languages
  - XCCDF: The Extensible Configuration Checklist Description Format
  - OVAL: Open Vulnerability and Assessment Language
  - OCIL: Open Checklist Interactive Language
  - Asset Identification
  - ARF: Asset Reporting Format
- Collections
  - CCE: Common Configuration Enumeration
  - CPE: Common Platform Enumeration
  - CVE: Common Vulnerabilities and Exposure
- Metrics:
  - CVSS: Common Vulnerability Scoring System
  - CCSS: Common Configuration Scoring System
- Integrity
  - TMSAD: Trust Model for Security Automation Data

OVAL, CCE, CPE and CVE are trademarks of NIST.

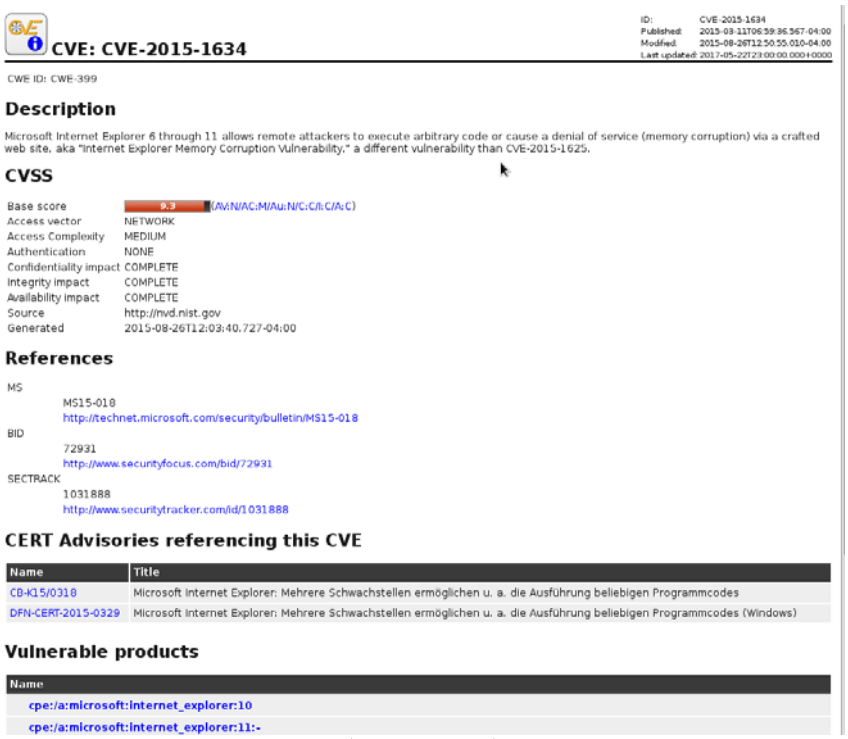
The Greenbone vulnerability scanner uses the OVAL standard, CVE, CPE and CVSS. By utilizing these standards the interoperability with other systems is guaranteed. These standards also allow comparing of the results.

Vulnerability scanners such as the Greenbone Security Manager can be validated by NIST respectively. The Greenbone Security Manager has been validated with respect to SCAP version 1.0 (https://nvd.nist.gov/scapproducts.cfm).

Following, the standards utilized by the Greenbone Security Manager are being covered in more detail.

9.8.3.1. CVE

Due to the fact that in the past often multiple organizations discovered and reported vulnerabilities at the same time and assigned them different names, communication and comparison of the results was not easy. Different scanners reported the same vulnerability under different names. As a matter of fact, instead of two different vulnerabilities it was actually the same vulnerability.



CVE: CVE-2015-1634

ID: CVE-2015-1634
Published: 2015-03-11T06:59:36.567-04:00
Modified: 2015-08-26T12:50:55.010-04:00
Last updated: 2017-05-22T23:00:00.000+0000

CWE ID: CWE-399

Description

Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1625.

CVSS

Base score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Access vector	NETWORK
Access Complexity	MEDIUM
Authentication	NONE
Confidentiality impact	COMPLETE
Integrity impact	COMPLETE
Availability impact	COMPLETE
Source	http://nvd.nist.gov
Generated	2015-08-26T12:03:40.727-04:00

References

MS
MS15-018
http://technet.microsoft.com/security/bulletin/MS15-018
BID
72931
http://www.securityfocus.com/bid/72931
SECTRACK
1031888
http://www.securitytracker.com/id/1031888

CERT Advisories referencing this CVE

Name	Title
CB-K15/0318	Microsoft Internet Explorer: Mehrere Schwachstellen ermöglichen u. a. die Ausführung beliebigen Programmcodes
DFN-CERT-2015-0329	Microsoft Internet Explorer: Mehrere Schwachstellen ermöglichen u. a. die Ausführung beliebigen Programmcodes (Windows)

Vulnerable products

Name
cpe:/a:microsoft:internet_explorer:10
cpe:/a:microsoft:internet_explorer:11:-

(_images/cve.png)

The CVEs include information regarding the severity and affected products.

To address this, MITRE [3], sponsored by the US-CERT, founded the CVE project in 1999. Every vulnerability is assigned a unique identifier consisting of the year and a simple number. This number then serves as central reference.

The CVE database of MITRE is not a vulnerability database. CVE was developed in order to connect the vulnerability database and other systems with each other. This allows for the comparison of security tools and services. This is why the CVE database does not contain any information regarding risk, impact or remediation of the vulnerability. Detailed technical information is also not included. A CVE only contains the identification number with status, a short description and references to reports and advisories.

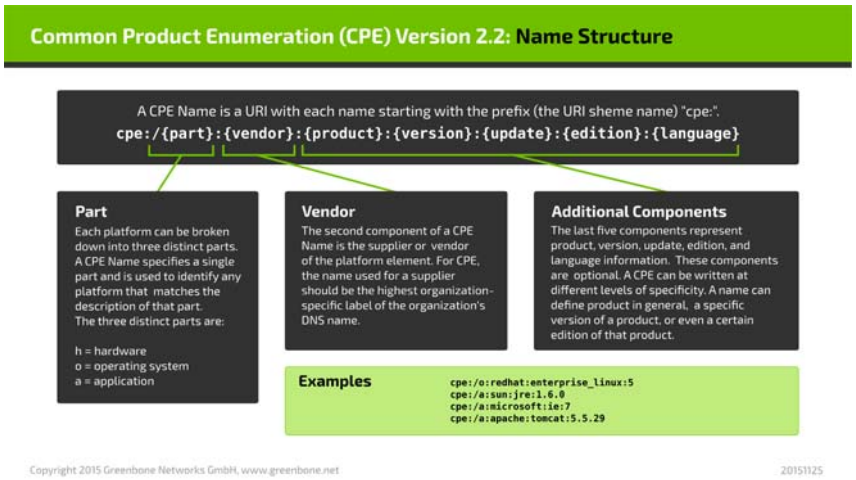
The National Vulnerability Database (NVD) refers to MITRE's CVE database and supplements this information with information in regard to remediation of the vulnerability, the severity, affected products and possible impact. Greenbone refers to the CVE database of the NVD so that information is included. At the same time does the GSM combine the information with the NVTs and the CERT-Bund and DFN-CERT advisories.

This information can be displayed comfortably in the web interface.

9.8.3.2. CPE

The abbreviation CPE stands for Common Platform Enumeration, modelled after CVE and started by MITRE as well, as an industry standard for a common naming convention for information technology systems. Hereby common naming exists for operating systems and applications allowing for global referencing.

Originally the Common Platform Enumeration (CPE) was initiated by MITRE. Today the CPE standard is maintained by the US American National Institute for Standards and Technology NIST as part of the National Vulnerability Database (NVD). NIST already had maintained the official CPE dictionary and the CPE specifications for many years. CPE is a structured naming schema for applications, operating systems and hardware devices. It is based on the generic syntax of the Uniform Resource Identifier (URI).



(_images/cpe_name_structure.png)

Common Product Enumeration: Name Structure

Due to the fact that the CPE standard is closely tied to the CVE standard, their combination allows for conclusion of existing vulnerabilities when discovering a platform or product.

CPE is composed of the following components:

Naming:

The name specification describes the logical structure of well-formed names (WFNs), its binding to URIs and formatted character strings and the conversion of the WFNs and their bindings.

Name Matching:

The name matching specification describes the methods to compare WFNs with each other. This allows for the testing if some or all refer to the same product.

Dictionary:

The dictionary is a repository of CPE names and metadata. Every name defines a single class of an IT product. The dictionary specification describes the processes for the use of the dictionary, like the search for a specific name or entries, which belong to a more general class.

Applicability Language:

The applicability language specification describes the creation of complex logical expressions with the help of the WFNs. These applicability statements can be used for the tagging of check lists, guide lines or other documentation and as such describe for which products these documents are relevant for.

9.8.3.3. OVAL

The Open Vulnerability and Assessment Language is also a Mitre project. It is a language to describe vulnerabilities, configuration settings (compliance), patches and applications (inventory). The XML based definitions allow for simple processing by automated systems. As such the OVAL definition `oval:org.mitre.oval:def:22127` of the inventory class describes the Adobe Flash Player 12 while the OVAL definition `oval:org.mitre.oval:def:22272` describes a vulnerability of Google Chrome under Windows.

OVAL Definition: oval:org.mitre.oval:def:22272

ID: oval:org.mitre.oval:def:22272
Created: 2014-02-03T12:56:06Z
Modified: 2014-03-17T08:00:17Z

Title:	Vulnerability in Google Chrome before 32.0.1700.76 on Windows allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog
Version:	4
Definition class:	vulnerability
Referenced CVEs:	1
Severity:	7.5
File:	oval/5.10/org.mitre.oval/v/family/windows.xml

Description

The OneClickSigninBubbleView::WindowClosing function in browser/ui/views/sync/one_click_signin_bubble_view.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog.

Affected

Family: windows

Type	Name
platform	Microsoft Windows 2000
platform	Microsoft Windows XP
platform	Microsoft Windows Server 2003
platform	Microsoft Windows Server 2008
platform	Microsoft Windows Server 2008 R2
platform	Microsoft Windows Vista
platform	Microsoft Windows 7
platform	Microsoft Windows 8
platform	Microsoft Windows 8.1
platform	Microsoft Windows Server 2012
platform	Microsoft Windows Server 2012 R2
product	Google Chrome

Criteria

- Google Chrome is installed (oval:org.mitre.oval:def:11914)

(_images/oval.png)

OVAL describes the discovery of vulnerabilities.

These OVAL definitions are created made available in XML and describe the discovery of individual systems and vulnerabilities. The above mentioned OVAL definition 22272 has the following structure:

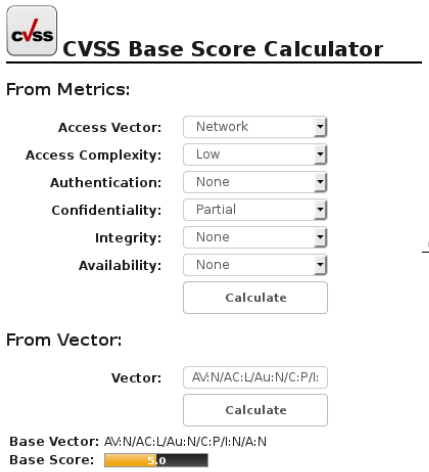
```
<definition id="oval:org.mitre.oval:def:22272" version="4" class="vulnerability">
  <metadata>
    <title>Vulnerability in Google Chrome before 32.0.1700.76 on Windows allows
           attackers to trigger a sync with an arbitrary Google account by
           leveraging improper handling of the closing of an untrusted signin
           confirm dialog</title>
    <affected family="windows">
      <platform>Microsoft Windows 2000</platform>
      <platform>Microsoft Windows XP</platform>
      <platform>Microsoft Windows Server 2003</platform>
      <platform>Microsoft Windows Server 2008</platform>
      <platform>Microsoft Windows Server 2008 R2</platform>
      <platform>Microsoft Windows Vista</platform>
      <platform>Microsoft Windows 7</platform>
      <platform>Microsoft Windows 8</platform>
      <platform>Microsoft Windows 8.1</platform>
      <platform>Microsoft Windows Server 2012</platform>
      <platform>Microsoft Windows Server 2012 R2</platform>
      <product>Google Chrome</product>
    </affected>
    <reference source="CVE" ref_id="CVE-2013-6643"
     ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6643"/>
    <description>The OneClickSigninBubbleView::WindowClosing function in
      browser/ui/views/sync/one_click_signin_bubble_view.cc in Google
      Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac
      OS X and Linux allows attackers to trigger a sync with an arbitrary
      Google account by leveraging improper handling of the closing of an
      untrusted signin confirm dialog.</description>
    <oval_repository>
      <dates>
        <submitted date="2014-02-03T12:56:06">
          <contributor organization="ALTX-SOFT">Maria Kedovskaya</contributor>
        </submitted>
        <status_change date="2014-02-04T12:25:48.757-05:00">DRAFT</status_change>
        <status_change date="2014-02-24T04:03:01.652-05:00">INTERIM</status_change>
        <status_change date="2014-03-17T04:00:17.615-04:00">ACCEPTED</status_change>
      </dates>
      <status>ACCEPTED</status>
    </oval_repository>
  </metadata>
  <criteria>
    <extend_definition comment="Google Chrome is installed"
     definition_ref="oval:org.mitre.oval:def:11914"/>
    <criteria operator="AND" comment="Affected versions of Google Chrome">
      <criterion comment="Check if the version of Google Chrome is greater than
        or equals to  32.0.1651.2" test_ref="oval:org.mitre.oval:tst:100272"/>
      <criterion comment="Check if the version of Google Chrome is less than
        or equals to  32.0.1700.75" test_ref="oval:org.mitre.oval:tst:99783"/>
    </criteria>
  </criteria>
</definition>
```


This information is being processed graphically by the web interface and presented easily readable (see figure OVAL describes the discovery of vulnerabilities.).

9.8.3.4. CVSS

A big problem for regular administrators is the interpretation of vulnerability with their own environment. How critical does he have to rate a vulnerability? To support personnel that do not work with the analysis and rating of vulnerabilities constantly the Common Vulnerability Scoring System (CVSS) was invented. CVSS is an industry standard for the description of the severity of security risks in computer systems. In the CVSS security risks are rated and compared using different criteria. This allows for the creation of a priority list of counter measures.

The CVSS score is continuously improved upon. Currently in general the CVSS score version 2 is being used. Version 3 is being developed by the CVSS Special Interest Group (CVSS-SIG) of the Forum of Incident Response and Security Teams (https://www.first.org/cvss) (FIRST).



(_images/cvss.png)

The CVSS calculator allows for the calculation of scores conveniently.

The CVSS score in version 2 supports Base Score Metrics, Temporal Score Metrics and Environmental Score Metrics.

The Base Score Metrics in general test the exploitability of a vulnerability and their impact on the target system. Hereby access, complexity and requirement of authentication are rated. At the same time they rate if the confidentiality, integrity or availability is threatened.

The Temporal Score Metrics test if completed example code exists, the vendor already supplied a patch and confirmed the vulnerability. The score will be changing drastically in the course of time.

The Environmental Score Metrics review if control damage has to be suspected, the target distribution, and if confidentiality, integrity of availability is required. This assessment is strongly depended on the environment in which the vulnerable product is being used.

Since the Base Score Metrics are merely meaningful in general and can be determined permanently the GSM provides them as part of the SecInfo data.

Hereby the following formula is being used and can be calculated with the CVSS calculator of the GSM as well (*Extras/ CVSS-Calculator*, see figure The CVSS calculator allows for the calculation of scores conveniently.):

```
BaseScore = roundTo1Decimal( ( ( 0.6 * Impact ) +
            ( 0.4 * Exploitability ) - 1.5 ) * f( Impact ) )
```

Hereby the impact is calculated as follows:

```
Impact = 10.41 * (1 - (1 - ConfImpact) *
         (1 - IntegImpact) * (1 - AvailImpact))
```

The exploitability is calculated as:

```
Exploitability = 20 * AccessVector * AccessComplexity * Authentication
```

The function `f( Impact )` is 0, if the impact is 0. In all other cases the value is 1.176. The other values are constants:

- Access Vector
  - requires local access: 0.395
  - adjacent network accessible: 0.646
  - network accessible: 1.0
- Access Complexity:
  - high: 0.35
  - medium: 0.61
  - low: 0.71
- Authentication
  - requires multiple instances of authentication: 0.45
  - requires single instance of authentication: 0.56
  - requires no authentication: 0.704
- ConfImpact:
  - none: 0.0
  - partial: 0.275
  - complete: 0.660
- IntegImpact
  - none: 0.0
  - partial: 0.275
  - complete: 0.660

- AvailImpact
  - none: 0.0
  - partial: 0.275
  - complete: 0.660

9.8.4. DFN-CERT

While the individual NVTs, CVEs, CPEs and OVAL definitions are being created primarily for processing by computer systems, the DFN-CERT publishes, like many other Computer Emergency Report Teams (CERTs), new advisories regularly.

The DFN-CERT is responsible for hundreds of universities and research institutions that are associated with the German Research Network (German: Deutsches Forschungsnetz, abbreviated as DFN). An Advisory describes especially critical security risks that require fast reacting. These are being obtained by the GSM as well and stored to the database for reference. They can be displayed directly as well.

9.8.5. CERT-Bund

CERT-Bund offers a warning and information service (German: Warn- und Informationsdienst, abbreviated as WID). Currently this service offers two different types of Information (Excerpt from the website https://www.cert-bund.de/ (https://www.cert-bund.de/)):

Advisories:

This information service is only available to federal agencies as a closed list! The advisories describe current information about security critical incidents in computer systems and detailed measures to remediate security risks.

Short Information:

Short information features the short description of current information regarding security risks and vulnerabilities. Please note that information sometimes is not verified and under some circumstances could be incomplete or even inaccurate.

The Greenbone Security Feed contains the CERT-Bund Short Information. They can be identified by the K in the message (`CB-K14/1296`).

Footnotes

[3] MITRE (Massachusetts Institute of Technology Research & Engineering) Corporation is an organization for the management of research institutions for the United States government that was formed by splitting off from the Massachusetts Institute of Technology (MIT).

Source (_sources/vulnerabilitymanagement.txt) Back to top

© Copyright 2015-2019, Greenbone Networks GmbH.
Created using Sphinx (http://sphinx-doc.org/) 1.3.5.