

# GSM: First Steps

## Content

- [First Scan: A single computer](#)

## Introduction

You have successfully finished the setup of the Greenbone Security Manager and have logged into the web interface for the first time.

Now it is time to take the first steps with this vulnerability management solution. In other words: it's time to run the first security scans of your IT infrastructure.



**Base rule:** Start with small scans and increase the scope step by step. You will learn about your network from the perspective of a vulnerability scanner.

Screenshots and descriptions refer to version 1.2 of the Greenbone Security Manager.

## First Scan: A single computer

1. Choose a computer on your network which you want to scan first. We need either its IP address (often an internal address for example starting with 192.168.) or its name (for example computer1.intern.company). In both cases you should ensure that the Greenbone Security Manager has access to this computer. When using names, a DNS service should be available.
2. Choose item "Targets" under Navigation and enter the address of the computer.

The screenshot shows the Greenbone Security Assistant web interface. At the top, it says 'Greenbone Security Assistant' and 'Logged in as training | Logout'. The date is 'Fri Jul 2 13:38:38 2010 (UTC)'. On the left is a navigation menu with categories like 'Scan Management', 'Configuration', 'Administration', and 'Help'. The main area is titled 'New Target' and contains a form with fields for 'Name' (My Desktop Computer), 'Comment (optional)', 'Hosts' (192.168.46.12), and 'Credential (optional)'. A 'Create Target' button is at the bottom right. Below the form is a 'Targets' table with columns for Name, Hosts, IPs, Credential, and Actions.

Name	Hosts	IPs	Credential	Actions
Localhost	localhost	1		 

You may add a comment. "Credentials" will be discussed later. Confirm now with "Create Target".

The screenshot shows the Greenbone Security Assistant interface. The top bar indicates the user is logged in as 'training' and the date is 'Fri Jul 2 13:55:16 2010 (UTC)'. The left navigation pane is expanded to 'Targets'. The main content area shows the 'Results of last operation' for 'Create Target' with a status code of 201 and a message 'OK, resource created'. Below this is the 'New Target' form with fields for Name (unnamed), Comment (optional), Hosts (localhost), and Credential (optional). A 'Create Target' button is visible. At the bottom, a 'Targets' table lists existing targets:

Name	Hosts	IPs	Credential	Actions
Localhost	localhost	1		[Edit] [Delete]
My Desktop Computer	192.168.46.12	1		[Edit] [Delete]

3. Choose "New Task" under Navigation. To create a task you need at least a name, a target and a scan configuration. The rest is optional. We created a target in the previous step. The GSM offers some pre-configured scan configurations of which "Full and fast" is an optimal "allrounder". This scan configuration is always recommended unless you want to apply intentionally a different scan behaviour.

The screenshot shows the Greenbone Security Assistant interface. The top bar indicates the user is logged in as 'training' and the date is 'Fri Jul 2 13:58:59 2010 (UTC)'. The left navigation pane is expanded to 'New Task'. The main content area shows the 'New Task' form with fields for Name (Scan my desktop), Comment (optional), Scan Config (Full and fast), Scan Targets (My Desktop Computer), Escalator (optional) (Localhost), and Schedule (optional). A 'Create Task' button is visible.

Confirm with "Create Task". The task gets created and the view changes to the task overview where you can see the newly created task with status "New".

Greenbone Security Assistant

Logged in as training | Logout  
Fri Jul 2 14:12:35 2010 (UTC)

Navigation

- Scan Management
  - Tasks
  - New Task
  - Notes
  - Performance
- Configuration
  - Scan Configs
  - Targets
  - Credentials
  - Escalators
  - Schedules
- Administration
  - Users
  - NVT Feed
  - Settings
- Help
  - Contents
  - About

Tasks Manual

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Scan my desktop	New						

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, [www.greenbone.net](http://www.greenbone.net)

4. Now click on the Icon (Start Task) and the scan begins.

Greenbone Security Assistant

Logged in as training | Logout  
Fri Jul 2 14:22:05 2010 (UTC)

Navigation

- Scan Management
  - Tasks
  - New Task
  - Notes
  - Performance
- Configuration
  - Scan Configs
  - Targets
  - Credentials
  - Escalators
  - Schedules
- Administration
  - Users
  - NVT Feed
  - Settings
- Help
  - Contents
  - About

Results of last operation

Operation: Start Task  
Status code: 202  
Status message: OK, request submitted

Tasks Manual

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Scan my desktop	Requested						

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, [www.greenbone.net](http://www.greenbone.net)

The status changes to "Requested". This means that the scan service is currently being told to run the scan. This all happens in the background and you can perform arbitrary other operations in the mean time, even run more tasks in parallel.

If you select "Tasks" under Navigation or the Icon (Refresh), then the progress information of all tasks will be updated.

Greenbone Security Assistant Logged in as training | Logout  
Fri Jul 2 14:22:35 2010 (UTC)

Navigation

- Scan Management
  - Tasks
  - New Task
  - Notes
  - Performance
- Configuration
  - Scan Configs
  - Targets
  - Credentials
  - Escalators
  - Schedules
- Administration
  - Users
  - NVT Feed
  - Settings
- Help
  - Contents
  - About

Tasks Manual

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Scan my desktop	4%	2				[Icons]	

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, [www.greenbone.net](http://www.greenbone.net)

Once the scan has started, the results that have been found so far can already be explored. Once the scan is finished, the status changes to "Done" and no further results will be added to the report.

Greenbone Security Assistant Logged in as training | Logout  
Fri Jul 2 14:26:19 2010 (UTC)

Navigation

- Scan Management
  - Tasks
  - New Task
  - Notes
  - Performance
- Configuration
  - Scan Configs
  - Targets
  - Credentials
  - Escalators
  - Schedules
- Administration
  - Users
  - NVT Feed
  - Settings
- Help
  - Contents
  - About

Tasks Manual

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Scan my desktop	Done	1		Jul 2 2010	High	[Icons]	

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, [www.greenbone.net](http://www.greenbone.net)

5. Congratulations! You have finished your first security scan with the Greenbone Security Manager.

You can click on the corresponding date in column "Last" to jump directly to the newest report of the corresponding task.

Greenbone Security Assistant Logged in as training | Logout  
Fri Jul 2 14:28:05 2010 (UTC)

**Navigation**

- Scan Management
  - Tasks
  - New Task
  - Notes
  - Performance
- Configuration
  - Scan Configs
  - Targets
  - Credentials
  - Escalators
  - Schedules
- Administration
  - Users
  - NVT Feed
  - Settings
- Help
  - Contents
  - About

**Report Summary** ?

**Result of Task:** Scan my desktop [Back to Task](#)

Order of results: by host

**Scan started:** Fri Jul 2 14:22:13 2010

Scan ended: Fri Jul 2 14:23:37 2010

Final scan run status: Done

Threat Counts:	11	22	19	10	Total 62

**Result Filtering**

Results 1 - 33 of 33 This report as: PDF | Download

Sorting: [port ascending](#) | [port descending](#) | [threat ascending](#) | threat descending

Show notes

Only show hosts that have results

CVSS >= 8.0

Text phrase:

Threat:  High  Medium  Low  Info  Info

[Apply](#)

**Filtered Results**

Host	Start	End	High	Medium	Low	Info	Total
<a href="#">192.168.46.12</a>	Jul 2, 14:22:13	Jul 2, 14:23:37	11	22	0	0	33
Total: 1			11	22	0	0	33

**Port summary for host "192.168.46.12"**

Service (Port)	Threat
http (80/tcp)	High
ssh (22/tcp)	Medium

**Security Issues reported for 192.168.46.12**

**High** http (80/tcp)

NVT: PHP 'solite\_single\_query()' and 'solite\_array\_query()' Arbitrary Code Execution... (OID: 1.3.6.1.4.1.25623.1.0.100631)

Overview:  
PHP is prone to multiple vulnerabilities that may allow

In the interactive report you can see 3 sections:

"Report Summary": Summarises the most relevant information for this report.

"Result Filtering": Here you can configure the filter that will be applied to the whole report to select the desired information or overviews. The default filter selects only the threat levels "High" and "Medium". The download always refers to the contents of the next section.


"Filtered Results": Shows the details of the vulnerability analysis corresponding to the configured filter.

You have now finished your first security scan with the Greenbone Security Manager and possibly found a number of vulnerabilities in you target system.

For understanding the report please note:

- The number of identified problems can be considerable. If a old version of, for example, PHP is installed, quite a number of tests will raise alerts. Once such a problematic piece of software is updated, the number of reported problems can drop significantly.

- Take actions for the results with threat level "High", then repeat the scan and work on the threat level "Medium". The levels "Low" and "Log" primarily help with in-depth analysis and require some in-depth knowledge.

Throughout the web interace you will find the help icon . Use this contextual online help to learn about the user options that have not been mentioned here.