

GSM: Erste Schritte

Inhalt

- Erster Scan: Ein einzelner Rechner

Einleitung

Sie haben das Setup des Greenbone Security Manager erfolgreich abgeschlossen und haben sich zum ersten mal an der Web-Oberfläche angemeldet.

Nun ist es soweit, dass die ersten Schritte mit unserer Schwachstellen-Management-Lösung gemacht werden können. Mit anderen Worten: die ersten Sicherheits-Scans Ihrer IT-Infrastruktur.

Als Grundregel gilt: Fangen Sie mit kleinen Scans an und steigern Sie den Umfang Schritt für Schritt. Sie werden Ihr Netzwerk aus Sicht eines Schwachstellen-Scanners neu kennenlernen.

Screenshots und Beschreibungen beziehen sich auf Version 1.2 des Greenbone Security Managers.

Erster Scan: Ein einzelner Rechner

1. Wählen Sie zunächst einen Rechner aus Ihrem Netz den Sie als erstes Scannen möchten. Sie benötigen entweder dessen IP-Adresse (zumeist ist das eine interne beginnend z.B. mit 192.168.) oder dessen Namen (z.B. rechner1.intern.company). In beiden Fällen sollte gewährleistet sein, dass der Greenbone Security Manager Zugang zu diesem Rechner hat. Bei Namen sollte der DNS-Dienst verfügbar sein.
2. Wählen Sie aus der Navigation den Punkt "Targets" und geben Sie die Adresse des Rechners an.

The screenshot shows the Greenbone Security Assistant web interface. At the top, it says 'Greenbone Security Assistant' and 'Logged in as training | Logout'. Below that, the date and time are shown: '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 content area is titled 'New Target' and contains a form with fields for 'Name' (filled with 'My Desktop Computer'), 'Comment (optional)', 'Hosts' (filled with '192.168.46.12'), and 'Credential (optional)'. A 'Create Target' button is at the bottom right of the form. Below the form is a table titled 'Targets' with columns for 'Name', 'Hosts', 'IPs', 'Credential', and 'Actions'. The table contains one entry: 'Localhost' with 'localhost' in the Hosts column, '1' in the IPs column, and a small icon in the Actions column.

Name	Hosts	IPs	Credential	Actions
Localhost	localhost	1		

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

Sie können auch gerne einen Kommentar angeben. Mit "Credentials" beschäftigen wir uns erst später. Bestätigen Sie nun mit "Create Target".

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

3. Wählen Sie aus der Navigation den Punkt "New Task". Für einen Task muss man mindestens einen Namen, ein Target und eine Scan Configuration angeben, der Rest ist optional. Ein Target haben wir soeben angelegt. Der GSM bietet ein paar voreingestellte Scan Configurations von denen "Full and Fast" als optimal eingestellter "Allrounder" immer verwendet werden sollte wenn man nicht bewusst ein anderes Scan-Verhalten anwenden möchte.

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

Bestätigen Sie mit "Create Task". Der Task wird angelegt und es wird zur Task-Übersicht gewechselt wo Sie den soeben erstellen Task mit dem Status "New" sehen.

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						[Play] [Refresh] [Stop] [Close] [Help]

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

4. Klicken Sie nun auf das Icon (Start Task) und der Scan beginnt.

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						[Refresh] [Play] [Stop] [Close] [Help]

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

Zunächst wechselt der Status auf "Requested". Das bedeutet, dass gerade der Scan-Dienst damit beauftragt wird den Scan-Task auszuführen. Das geschieht im Hintergrund und Sie können im Prinzip beliebige andere Aktionen ausführen, durchaus z.B. auch weitere Scan parallel starten.

Wenn Sie in der Navigation "Tasks" anwählen oder das Icon (Refresh), dann wird die Fortschritts-Information aller Tasks aktualisiert.

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%	1					

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

Hat der Scan einmal begonnen, kann übrigens zu jedem Zeitpunkt bereits der Report zu den bisher ermittelten Ergebnissen eingesehen werden. Ist der Scan abgeschlossen, ändert sich der Status auf "Done". Nun kommen keine weitere Resultate mehr dazu.

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		

Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

5. Herzlichen Glückwunsch! Sie haben Ihren ersten Schwachstellen-Scan mit dem Greenbone Security Manager abgeschlossen.

Um direkt in den zuletzt erstellten Report eines Task zu wechseln kann man in der Spalte "Last" auf den entsprechenden Datums-Eintrag klicken.

The screenshot displays the Greenbone Security Assistant interface. At the top, it shows the user is logged in as 'training' and the date is 'Fri Jul 2 14:28:05 2010 (UTC)'. The interface is divided into several sections:

- Navigation:** A sidebar menu with categories like Scan Management, Configuration, Administration, and Help.
- Report Summary:** Shows the task name 'Scan my desktop', scan dates, and a bar chart of threat counts: 11 Critical, 22 High, 19 Medium, 10 Low, and a total of 62.
- Result Filtering:** Allows filtering results (1-33 of 33) by sorting (port ascending) and showing only hosts with results. A CVSS filter is set to >= 8.0.
- Filtered Results:** A table showing results for host 192.168.46.12, including a port summary and a security issue for 'http (80/tcp)' with a high severity.

Im interaktiven Report sehen Sie nun 3 Unter-Bereiche:

"Report Summary": Fasst die wichtigsten Informationen die zu diesem Report gehören zusammen.

"Result Filtering": Hier wird ein Filter eingestellt der auf den gesamten Report angewendet wird um die gewünschten Informationen bzw. Übersichten herauszusuchen. In der Voreinstellung werden nur die Bedrohungen der Stufen "High" und "Medium" angezeigt. Der zuletzt angewandte Filter wird auch immer für den Download der verschiedenen Formate benutzt.

"Filtered Results": Zeigt die Details des Reports mit den einzelnen Ergebnissen der Schwachstellen-Analyse.

Sie haben nun den ersten Sicherheits-Scan mit dem Greenbone Security Manager abgeschlossen und möglicherweise ein paar Schwachstellen für das Zielsystem gefunden.

Zum Verständnis des Report beachten Sie bitte:

- Die Zahl der gefundenen Probleme kann durchaus nennenswert sein. Ist aber eine veraltete Version z.B. von PHP installiert, so schlagen natürlich eine ganze Reihe verschiedener Tests gleichzeitig

Alarm. Wird eine solche problematische Software aktualisiert, so kann die Anzahl der berichteten Probleme deutlich sinken.

- Kümmern Sie sich bei den Maßnahmen zunächst um die Meldungen der Bedrohungsstufe "High" und wiederholen Sie den Scan bevor Sie sich der Stufe "Medium" zuwenden. Die Stufen "Low" und "Log" dienen vor allem dem Detail-Verständnis und erwarten eben solches für die Interpretation.

Überall in der Web-Oberfläche finden Sie das Hilfe-Icon . Nutzen Sie diese kontext-bezogene Online-Hilfe um sich mit den hier nicht weiter erwähnten Anwender-Optionen vertraut zu machen.