

Feature: Report Formats

Inhalt

- [Report Formats organisieren](#)
- [Report Formats verwenden](#)

Einleitung







































Die [Report Format Plugins](#) stellen eine sehr mächtige Funktionalität dar. Aus einem Scan-Ergebnis erstellen sie Detail-Berichte in verschiedenen Formaten, Zusammenfassungen, Exportformate, graphische Übersichten und sogar kleine in sich geschlossene Programme die einer interaktive Analyse der Ergebnisse erlauben.

Darüber hinaus sind einige Plugins konfigurierbar. Dies erlaubt eine Feineinstellung des gewünschten Verhaltens, wie z.B. die Größe einer zu erstellenden Graphik.

Wir haben eine [Übersicht zu voreingestellten und importierbaren Report Format Plugins](#) die durch den Greenbone Security Manager unterstützt werden zusammengestellt. Sie wird permanent erweitert. Auch der [Greenbone Security Explorer](#) ist ein Plugin und wird von Greenbone individuell für Kunden konfiguriert.

Report Formats organisieren

Eine Übersicht über alle verfügbaren Report Format Plugins erhält man über die Navigation unter "Configuration->Report Formats":


Name	Extension	Content Type	Trust (last verified)	Active	Actions
CPE (Common Product Enumeration CSV table.)	csv	text/csv	unknown (Jan 24 2011)	yes	    
HTML (Single page HTML report.)	html	text/html	unknown (Jan 24 2011)	yes	    
ITG (German "IT-Grundschutz-Kataloge" report.)	csv	text/csv	unknown (Jan 24 2011)	yes	    
LaTeX (LaTeX source file.)	tex	text/plain	unknown (Jan 24 2011)	yes	    
NBE (Legacy OpenVAS report.)	nbe	text/plain	unknown (Jan 24 2011)	yes	    
PDF (Portable Document Format report.)	pdf	application/pdf	unknown (Jan 24 2011)	yes	    
TXT (Plain text report.)	txt	text/plain	unknown (Jan 24 2011)	yes	    
XML (Raw XML report.)	xml	text/xml	unknown (Jan 24 2011)	yes	    

Diese Liste zeigt die voreingestellten Plugins bei Auslieferung des GSM (Version 1.4). Jedes Plugin hat die folgenden Eigenschaften:

- **Extension:** Der Dateiname für den heruntergeladenen Bericht über das jeweilige Plugin besteht aus der UUID (eindeutige interne ID des Berichts) und dieser Extension. Die Extension hilft unter Anderem dem Browser eine passende Anwendung zu starten falls der Content Type dafür nicht ausreicht.
- **Content Type:** Die Kennungen entsprechen dem HTML-Standard und werden beim Download auch entsprechend mitgesendet um den Start der passenden Anwendung zu unterstützen.

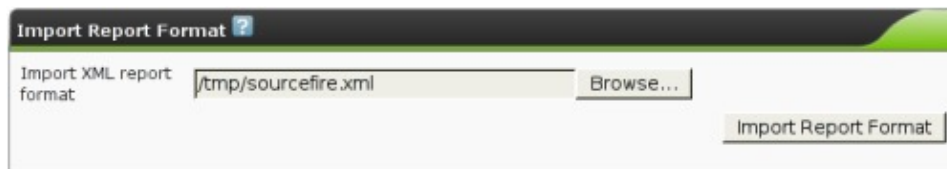
Darüber hinaus ist der Content Type aber auch intern von Bedeutung: Er wird benutzt um jeweils im Kontext passende Plugins zur Auswahl anzubieten. Beispielsweise werden für die Eskalation via Email alle Plugins des Typs "text/*" angeboten, da diese direkt lesbar in den Email-Textbereich eingebettet werden können.

- **Trust:** Einige Plugins bestehen lediglich aus einer Datentransformation während andere einige komplexere Operation ausführen und dabei auch Hilfsprogramme verwenden. Um einen Mißbrauch zu vermeiden, lassen sie Plugin digital signieren. Ist die Signatur authentisch und vertrauen Sie dem Aussteller, so ist sichergestellt, dass sie das Plugin in genau der vom Aussteller zertifizierten Form vorliegen haben.

Die Prüfung erfolgt nicht automatisch sondern manuell über das -Icon. Das Datum dieser Prüfung wird dann automatisch gesetzt. Diese Funktion sollte unbedingt immer für neu importierte Plugins angewendet werden bevor sie aktiviert werden.

- **Active:** Die Plugins stehen nur dann in den jeweiligen Auswahllisten zur Verfügung wenn sie aktiviert wurden. Neu importierte Plugins sind zunächst immer deaktiviert.

Ein neues Plugin wird wie folgt importiert. Es wird angenommen, dass Sie das Plugin bereits heruntergeladen und im Verzeichnis für temporäre Dateien abgelegt haben.





Nach erfolgreichem Import taucht das neue Plugin in der Liste auf. Es ist deaktiviert und da es kein voreingestelltes Plugin ist, kann es natürlich auch wieder gelöscht werden.

PDF (Portable Document Format report.)	pdf	application/pdf	unknown (Jan 24 2011)	yes	    
Sourcefire (Sourcefire Host Input Import.)	csv	text/csv	unknown (Mar 21 2011)	no	    
TXT (Plain text report.)	txt	text/plain	unknown (Jan 24 2011)	yes	    

Prüfen Sie vor der Aktivierung zunächst die Vertrauenswürdigkeit des Plugins:

PDF (Portable Document Format report.)	pdf	application/pdf	unknown (Jan 24 2011)	yes	    
Sourcefire (Sourcefire Host Input Import.)	csv	text/csv	yes (Mar 21 2011)	no	    
TXT (Plain text report.)	txt	text/plain	unknown (Jan 24 2011)	yes	    

Gehen Sie nun in den Bearbeitungsmodus über das -Icon und aktivieren Sie das Plugin.



Edit Report Format ?

Name:

Summary:

Active: yes no

Parameters: None

Nun taucht es in den passenden Plugin-Auswahlen auf.

Report Formats verwenden

In der interaktiven Report-Ansicht des Greenbone Security Assistant werden sämtliche aktivierten Plugins zur Auswahl angeboten:



Report Summary ?

Result of Task: Test scan [Back to Task](#)

Order of results: by host

Scan started: **Mon Mar 21 12:31:05 2011**

Scan ended:

Scan status: 

	High	Medium	Low	Info	Errors	Total	Download
Full report:	0	2	11	9	0	22	PDF 
All filtered results:	0	2	0	0	0	2	CPE  HTML  ITS  LaTeX  NBE  PDF  Sourcefire  TXT  XML 
Filtered results 1 - 2:	0	2	0	0	0	2	

Result Filtering

Sorting: [port_ascending](#) | [port_descending](#) | [threat_ascending](#) | [threat_descending](#)

Als Inhalt für eine automatisch verschickte Email werden nur diejenigen Plugins angeboten die ein Textformat anbieten:

New Escalator ?

Name

Comment (optional)

Event Task: run status changed to

Condition Always
 Threat level is at least
 Threat level

Method Email
To Address
From Address
Content Simple notice
 Include report:

System Logger (Syslog)
 SNMP
 HTTP Get
URL

Weitere Beispiele für die Verwendung spezieller Plugins finden sich hier:

- **ITG: IT-Grundschatz**