

GSM: IDS Optimierung

Inhalt

- [Vorbereitung des Sourcefire Defense Centers](#)
- [Konfiguration des Greenbone Security Manager](#)
- [Ergebnis an das Sourcefire Defense Center übertragen](#)
- [Ergebnisse im Sourcefire Defense Center ansehen](#)

Einleitung

Netzwerk-basierte Intrusion Detection Systeme (NIDS) haben die Aufgabe Angriffe gegen das Netzwerk zu identifizieren und zu melden. Sie schneiden dafür den Netzwerkverkehr mit und analysieren diesen auf verdächtige Aktivitäten hin. Dies schließt die Identifikation auch komplexer Angriffsmuster ein.

In der Regel ist die IDS-Funktion mit einem Intrusion Prevention System (IPS) gekoppelt. Damit kann unmittelbar auf eine Bedrohung reagiert werden, zum Beispiel in dem Datenpakete gelöscht werden, Verbindungen unterbrochen werden oder die übertragenen Daten so geändert werden dass die davon ausgehende Gefahr beseitigt wird.

Eine optimale Leistung kann das NIDS/IPS dann erbringen wenn der gesamte Datenstrom erfasst wird. Damit wird es aber zum Flaschenhals der Netzwerkinfrastruktur und jegliche Optimierung erhöht den Datendurchsatz.

Genau hier kommt der Greenbone Security Manager ins Spiel: Im Gegensatz zum passiven, also auf Angriffe wartenden NIDS/IPS, hat der GSM aktiv Informationen zu schwachen Systemen der IT-Infrastruktur gesammelt. Seine Daten helfen dem NIDS/IPS die Arbeit zu optimieren, beispielsweise gefährdete Systeme mit Priorität zu behandeln.

- **GSM-NIDS/IPS Kopplungsmethode 1: Manueller Daten-Transfer von GSM nach NIDS/IPS**

Jeder beliebige Bericht zu einem Schwachstellen-Scan kann an das NIDS/IPS gesendet werden. Entweder per Export/Import (bei unbekanntem oder nicht erreichbarem NIDS/IPS) oder aber auch auf einen einfachen Knopfdruck hin (wenn GSM und das NIDS/IPS miteinander bekannt gemacht wurden).

Der Anwender kann vollständige Berichte senden oder einen nach beliebigen Kriterien gefilterten Bericht.

- **GSM-NIDS/IPS Kopplungsmethode 2: Automatischer Daten-Transfer von GSM nach NIDS/IPS**

Sind GSM und NIDS/IPS füreinander konfiguriert, so ist der Daten-Transfer von GSM nach NIDS/IPS so einfach wie jede andere Eskalations-Routine beim GSM. Nach Abschluss eines Scans wird entsprechend der gewünschten Kriterien das Scan-Ergebnis ganz automatisch an das NIDS/IPS übertragen. Läßt man diesen Scan-Auftrag jede Woche automatisch ausführen erhält man ein

vollautomatisiertes Melde- und Optimierungssystem.

- **GSM-NIDS/IPS Kopplungsmethode 3: Aktive Steuerung des GSM durch NIDS/IPS**

Beim Betrieb des NIDS/IPS entstehen Verdachtsmomente zu Systemen mit besondere Gefährdung. Der GSM kann für eine Inspektion dieser speziellen Systeme beauftragt werden. Sobald er mit seiner Arbeit fertig ist, sendet er von allein seine Ergebnisse zurück. In der Zwischenzeit arbeiten beide Systeme vollkommen unabhängig voneinander weiter, keines blockiert das andere.

Sind GSM und NIDS/IPS erst einmal aufeinander eingestellt, bedarf es dann keinerlei manueller Arbeit mit dem GSM. Das NIDS/IPS steuert den gesamten Ablauf des GSM.

Folgende NIDS/IPS werden direkt von Greenbone unterstützt:

- Sourcefire Defense Center (ab GSM 1.5)

Eine Schritt-für-Schritt Anleitung für dieses Produkt finden Sie auf dieser Seite.

Vorbereitung des Sourcefire Defense Centers

Damit Ihr Sourcefire Defense Center Ergebnisse von einem Greenbone Security Manager (GSM) entgegennimmt, müssen Sie zunächst den GSM im Defense Center als so genannten Host Input Client anlegen und ein entsprechendes Zertifikat erstellen.

Begeben Sie sich dazu in das Konfigurationsmenü der Host Input Clients, das unter "Operations" und dort unter "Configuration" finden. Klicken Sie in diesem Konfigurationsmenü auf "Create Client" und geben Sie die IP oder den Namen Ihres GSMs ein. Ein Passwort muss nicht eingegeben werden.



Nach der Erstellung des Host Input Clients können Sie nun das Zertifikat herunterladen, indem Sie auf den in der Spalte "Certificate Location" genannten Link klicken. Speichern Sie dieses Zertifikat lokal ab.



Hostname	Certificate Location
192.168.11.56	http://kava:bastrop4_clients/192.168.11.56/ob-12

Konfiguration des Greenbone Security Manager

Auf dem GSM benötigt man das Report Format Plugin "Sourcefire Host Input Import". Falls noch nicht installiert, findet man es bei den [Report Format Downloads](#). Das Report Format Plugin können Sie installieren, indem Sie auf Ihrem GSM das Menü "Report Formats" öffnen, dort unter "Import Report Format

Plugin" das von Ihnen heruntergeladene Plugin auswählen und auf "Import Report Format" klicken. Das Plugin erscheint nun in der Liste der Report Formats.

NBE (Legacy OpenVAS report.)	nbe	text/plain	yes (May 27 2011)	yes	
PDF (Portable Document Format report.)	pdf	application/pdf	yes (May 27 2011)	yes	
Sourcefire (Sourcefire Host Input Import.)	csv	text/csv	yes (May 30 2011)	no	
TXT (Plain text report.)	txt	text/plain	yes (May 27 2011)	yes	
XML (Raw XML report.)	xml	text/xml	yes (May 27 2011)	yes	

Um das Report Format Plugin nutzen zu können, müssen Sie es aktivieren. Stellen Sie zunächst sicher, dass das Plugin vertrauenswürdig ist: In der Spalte "Trust" muss der Wert "yes" erscheinen. Klicken Sie dann auf das -Symbol und setzen Sie die Einstellung "Active" auf "yes". Klicken Sie auf die Schaltflächen "Save Report Format", um diese Einstellung zu speichern.

Edit Report Format ?

Name

Summary

Active yes no

Parameters: None

Als nächstes legen Sie einen Escalator an, der Ihren GSM mit dem Sourcefire Defense Center verbindet. Öffnen Sie hierzu das Menü "Escalators" und erstellen Sie einen neuen Escalator. Nachdem Sie einen Namen für den Escalator festgelegt haben, wählen Sie bei "Method" den Typ "Sourcefire Connector". Tragen Sie in die dazugehörigen Eingabefelder die IP und den Port Ihres Defense Centers ein und wählen Sie für das Feld "PKCS12 file" das Zertifikat aus, welches Sie zuvor vom Sourcefire Defense Center heruntergeladen haben.

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:

Sourcefire Connector
 Defense Center IP:
 Defense Center Port:
 PKCS12 file:

Ergebnis an das Sourcefire Defense Center übertragen

Um einen bestehenden Report an das Sourcefire Defense Center zu übertragen, öffnen Sie zunächst den Report. Im Report Summary können Sie nun den gesamten Report oder eine gefilterte Auswahl übertragen, indem Sie in der entsprechenden Zeile in der Spalte "Escalate" den von Ihnen soeben erstellten Escalator auswählen und auf das -Symbol klicken.

	High	Medium	Low	Log	False Pos.	Total	Escalate	Download
Full report:	11	22	19	10	0	62	Sourcefire DC	PDF
All filtered results:	11	22	0	0	0	33	Sourcefire DC	PDF
Filtered results 1 - 33:	11	22	0	0	0	33	Sourcefire DC	PDF

Sie können, wie jeden anderen Escalator auch, den Sourcefire Connector so einsetzen, dass Scan-Ergebnisse automatisch an das Defense Center übertragen werden. Wählen Sie hierzu einfach den von Ihnen erstellten Escalator aus, wenn Sie einen neuen Task erstellen oder wählen Sie den Escalator für einen bestehenden Task aus, indem in der Task-Übersicht auf das -Symbol klicken.

New Task ?

Name: Scan Webserver and report to DC

Comment (optional): e result to the Sourcefire Defense Center

Scan Config: Full and fast

Scan Targets: Webserver

Escalator (optional): Sourcefire DC

Schedule (optional): --

Slave (optional): --

Create Task

Es ist ebenfalls möglich, die Ergebnisse eines Scans nur zu übertragen, wenn bestimmte Bedingungen erfüllt sind; diese Bedingungen können Sie bei der Erstellung des Escalator setzen und den neu erstellten Escalator dann bei Ihrem Tasks einsetzen.

New Escalator ?

Name: Threat Increase to Sourcefire DC

Comment (optional): e Center if the Threat level has increased

Event: Task: run status changed to Done

Condition: Always
 Threat level is at least High
 Threat level increased

Ergebnisse im Sourcefire Defense Center ansehen

Im Sourcefire Defense Center können Sie die übertragenen Ergebnisse unter dem Menüpunkt "Analysis & Reporting: RNA" und dort unter "RNA Events" einsehen. In den Daten zu den von Ihnen übertragenen Zielsystemen finden Sie nun einen Abschnitt, der die vom GSM identifizierten Schwachstellen enthält.

Scan Vulnerability Detail

Scan Type:	OpenVAS
Vulnerability ID:	1
Name:	Check SSL Weak Ciphers and Supported Ciphers
Description:	Server will not supports SSLv2 Ciphers. Server will not supports SSLv3 Ciphers. Server will not supports TLSv1 Ciphers. None of the weak ciphers are supported.
BugTraq ID:	0
CVE ID:	NOCVE