

OMP Fernsteuerung

Inhalt

- [Fernsteuerung aktivieren](#)
- [Funktionsweise der Fernsteuerung](#)
- [Einfache Beispiele](#)
- [Beispiel: Local Security Checks passiv ausführen](#)

Einleitung

Der Greenbone Security Manager bietet eine Fernsteuerung über das SSL-gesicherte Protokoll "OMP". Mit OMP verfügt man über den gleichen Funktionsumfang wie ihn die Web-Oberfläche bietet. Wenn Sie selbst einen OMP-Client für den Greenbone Security Manager implementieren möchten, nutzen Sie die umfangreiche englische [OMP 3.0 Spezifikation](#). Beachten Sie bitte, dass die unten beschriebenen Beispiele sich auf OMP 2.0 beziehen und für ältere Version leicht abweichen können. Bitte nehmen Sie ggf. Kontakt mit unserem Support-Team auf.

Sie müssen das Protokoll aber nicht selbst implementieren. Greenbone Networks bietet allen Kunden kostenlos an, das OMP Kommandozeilen-Werkzeug für das gewünschte Betriebssystem bereitzustellen. Das Kommandozeilen-Werkzeug ist für eine Vielzahl von GNU/Linux-Distributionen verfügbar. Die [Greenbone Desktop Suite](#) für Microsoft Windows enthält ebenfalls das Kommandozeilen-Werkzeug. Falls das Kommandozeilen-Werkzeug auf Ihrem Betriebssystem nicht verfügbar ist, wenden Sie sich einfach mit Ihrer Kundennummer, dem benötigten Betriebssystem und einer kurzen Übersicht welche Aufgaben Sie über Fernsteuerung erledigen wollen an den technischen Support (siehe [Kontakt](#)).

Fernsteuerung aktivieren

Per Voreinstellung ist die Fernsteuerung beim GSM zunächst deaktiviert.

Loggen Sie sich als Administrator auf der CLI-Admin-Oberfläche ein (siehe auch Handbuch "GSM Command Line Interface: Administrator Guide") und aktivieren Sie die OMP Schnittstelle wie folgt. **Beachten Sie**, dass ein Neustart des GSM notwendig ist um die Änderung zu aktivieren.

```
gsm> set public_omp enabled
gsm *> commit
gsm> reboot
```

Analog lässt sich die Fernsteuerung natürlich wieder ausschalten:

```
gsm> set public_omp disabled
gsm *> commit
gsm> reboot
```

Funktionsweise der Fernsteuerung

Das Protokoll OMP ist XML-basiert. Jedes Kommando und jede Antwort ist also ein XML Objekt.

Das von Greenbone Networks gelieferte Kommandozeilen-Werkzeug "omp" bietet zum einen das direkte Versenden und Empfangen von XML-Kommandos und XML-Antworten. Das ist vor allem für den Batch-Betrieb ("Stapelverarbeitung", "Scripting") hilfreich. Zum anderen sind die wichtigsten Kommandos als Kommandozeilenparameter abgebildet sowie eine Option für gut lesbare Ausgabe verfügbar. Dies ist gedacht für spontane Abfragen, Tests und zur Ausbreitung von Batch-Prozessen.

Grundsätzlich bietet das Kommandozeilen-Werkzeug "omp" zwei Arten der Verwendung an. Über den Schalter "--xml" werden OMP-Kommandos im XML Format gesendet. Die Antworten sind dann ebenfalls im XML Format. Einige der Kommandos sind ebenfalls als direkte Schalter verfügbar. So entspricht "--xml=" dem Schalter "--get-tasks". Bei Verwendung von letzterem erfolgt die Ausgabe aber nicht im XML-Format sondern als einfache Text-Tabelle.

Einfache Beispiele

Diese Beispiele verwenden eine klassische Unix-Shell. Entsprechend lassen sich die Aufrufe auch in andere Anwendungen bzw. Umgebungen integrieren.

Zur Vereinfachung werden zunächst die Verbindungsdaten in der Datei "omp.config" im Heimatverzeichnis des Anwenders hinterlegt. Unter Unix-ähnlichen Systemen ist das "\$ (HOME)/omp.config" und unter Windows-System "%USERPROFILE%\omp.config". Erstellen Sie diese Datei mit folgendem Inhalt (host, username und password sind natürlich entsprechend anzupassen und achten Sie auf korrekte Groß-Kleinschreibung):

```
[Connection]
host=gsm
port=9390
username=demouser
password=demouser
```

Achten Sie darauf, dass diese Datei nur Ihnen lesend und schreibend zugänglich ist bevor Sie die echten Verbindungsdaten eintragen (unter Unix-ähnlichen Systemen z.B. via "touch omp.config && chmod 600 omp.config").

Übersicht zu den existierenden Tasks des Benutzers in formatierter XML-Ansicht:

```
omp --pretty-print --xml="<get_tasks/>"
```

Übersicht zu den Kommandozeilen-Parametern von "omp":

```
omp --help
```

Übersicht zu den verfügbaren OMP Kommandos des angesprochenen GSM:

```
omp --xml="<help/>"
```

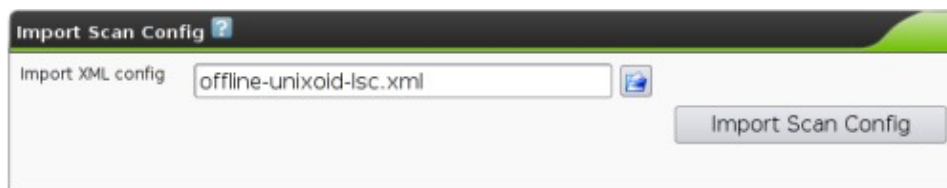
Beispiel: Local Security Checks passiv ausführen

Dieses Beispiel illustriert die Mächtigkeit des Fernsteuerungs-Features besonders gut: Es wird erreicht, dass für ein Zielsystem die Local Security Checks ausgeführt werden ohne dass der GSM das Zielsystem überhaupt aktiv anspricht, geschweige denn Information zu dessen IP hat oder es auch nur über das Netzwerk erreichen könnte.

Vorbereitung der Scan Configuration

Dieser Schritt muss nicht für jeden Scan ausgeführt werden sondern nur pro gewünschter Scan Configuration. In diesem Beispiel für den Offline-LSC-Scan von unixoide Systemen (Linux, Solaris, HP-UX).

Importieren Sie die Scan Configuration Offline Unixoid LSC:



Scan ausführen

Dieses Beispiel verwendet eine klassische Unix-Shell. Entsprechend lassen sich die Aufrufe auch in andere Anwendungen bzw. Umgebungen integrieren.

1. Initialisierung über Variablen ausführen:

```
SCANCONFIG_NAME="Offline Unixoid LSC"  
TASK_NAME="Offline LSC Scan RHEL5"  
AUDIT_FILE="rhel5_example.audit"
```

SCANCONFIG_NAME: Muss identisch sein mit einer vorhandenen Scan Configuration.

TASK_NAME: Kann beliebig gewählt werden.

AUDIT_FILE: Ein auf einem Zielsystem erstellte Audit-Datei, z.B. über gb-lsc-agent. Zum Ausprobieren können Sie obiges Beispiel herunterladen.

2. Task anlegen:

```
TASK_UUID=`omp -c "$SCANCONFIG_NAME" -C --name "$TASK_NAME" -t Localhost`  
iconv -f latin1 -t UTF-8 $AUDIT_FILE | sed 's/\\n;/g' | omp \  
  --modify-task $TASK_UUID --file --name /tmp/results.lsc
```

3. Task starten:

```
REPORT_UUID=`omp --start-task $TASK_UUID`
```

4. Auf das Ende des Scans warten:

Mit folgendem Aufruf erhält man den Status des Tasks:

```
omp --get-tasks $TASK_UUID
```

Der Scan ist abgeschlossen wenn der Status "Done" erreicht ist.

96ebc7e4-d63d-405b-a21b-af20cf787bcd Done

Offline LSC Scan RHEL5

5. Bericht in gewünschtem Format abholen:

```
omp --get-report $REPORT_UUID --format 1a60a67e-97d0-4cbf-bc77-f71b08e7043d > report.pdf
```

Die entsprechende REPORT_UUID hat man beim Start des Scans erhalten.

Die Zeichenkette "1a60a67e-97d0-4cbf-bc77-f71b08e7043d" beschreibt das Format welches genutzt werden soll, in diesem Fall PDF. Sie können mit dem folgenden Befehl die Liste der verfügbaren Formate abrufen:

```
omp --get-report-formats
```

6. Aufräumen:

```
omp --delete-task $TASK_UUID
```

Die entsprechende TASK_UUID hat man beim Erstellen des Tasks erhalten.