

# Task: Nmap Skripte ausführen

## Inhalt

- [Einfache Netzwerkscans mit NSE](#)
- [Ausführen des Scans](#)
- [Anpassung der Parameter](#)

## Einleitung

Nmap ist das bei Sicherheitsexperten am weitesten verbreitete Werkzeug zur Erforschung und Untersuchung von Netzwerken. Nmap enthält Unterstützung für die Skriptsprache LUA und beinhaltet dutzende Skripte für die Identifikation von Systemen und Diensten.

Greenbone Security Manager (GSM) integriert Nmap als festen Bestandteil für die Phase der Netzwerk-Bestandsaufnahme. Für Sicherheits-Experten stellt der GSM auch die spezielleren Möglichkeiten von Nmap zur Verfügung wie zum Beispiel die NSE-Skripte.

Der Greenbone Security Manager erlaubt es, durch die Benutzung der Nmap Scripting Engine (NSE) die Ergebnisse einer Netzwerkuntersuchung zu erweitern. Dadurch ist es möglich, die Ergebnisse von NSE-Skripten auf die gleiche Weise zu verwalten wie die Ergebnisse von NVTs, wie z.B. in Bezug auf Anmerkungen, Filter und Berichte.

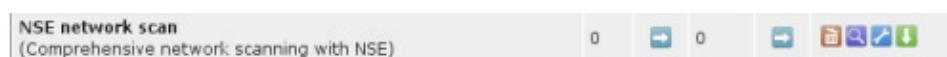
## Einfache Netzwerkscans mit NSE

Sie können die Datei [nmap-nse.xml](#) importieren und erhalten dann direkt eine lauffähige Scan Configuration. Falls Sie sich dazu entscheiden, können Sie die nachfolgenden Schritte überspringen und direkt mit dem [Ausführen des Scans](#) fortfahren.

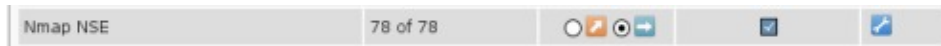


Im nächsten Schritt erstellen wir eine neue leere Scan Configuration und aktivieren NSE von Hand um die Vorgehensweise zu veranschaulichen. In den voreingestellten Konfigurationen sind die NSE-Skripte zwar enthalten, werden aber standardmäßig nicht ausgeführt.

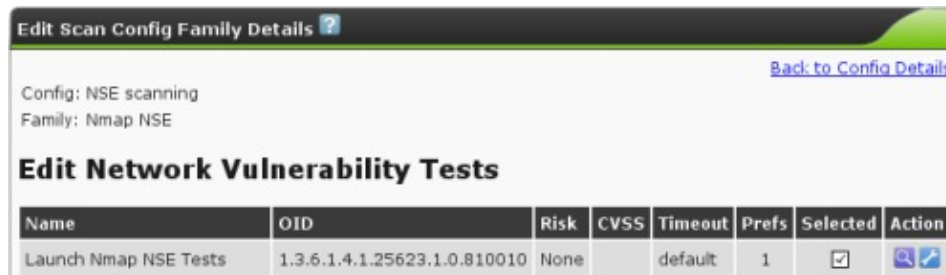
Klicken Sie auf , um Ihre Konfiguration zu bearbeiten.



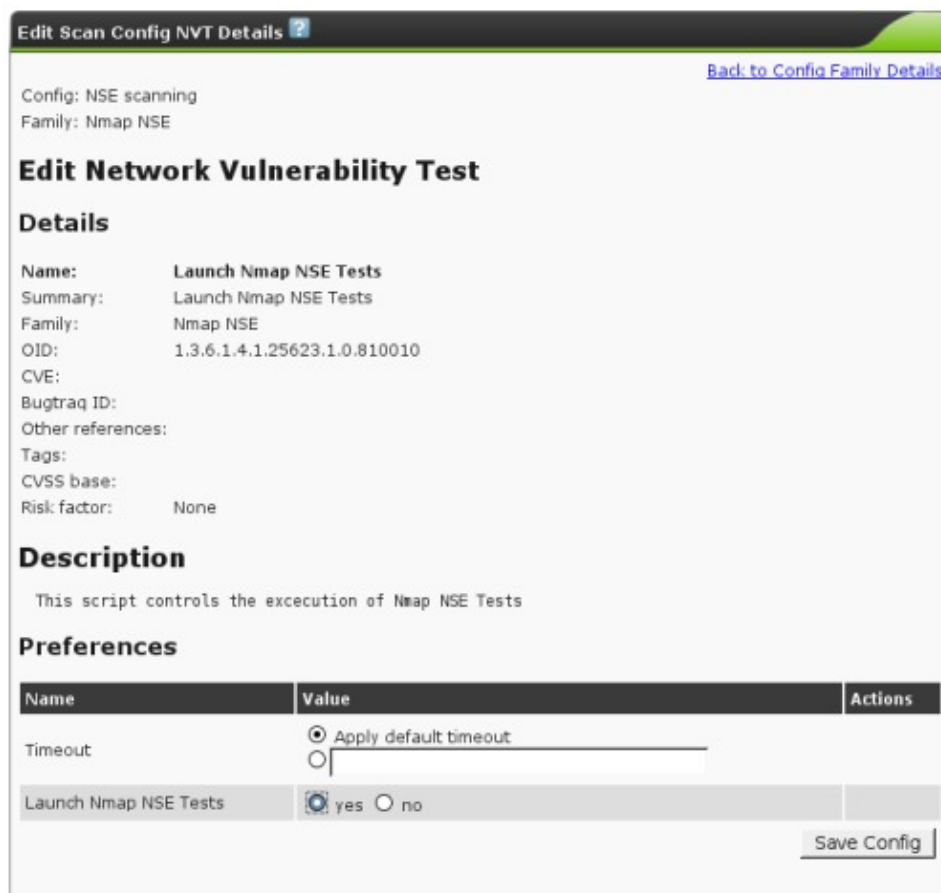
Wählen Sie die Familie (family) *Nmap NSE* aus, um die NSE-Skript für diese Konfiguration auszuwählen. Speichern Sie die Konfiguration.



NSE-Skripte werden nun für den Scan berücksichtigt. Sie werden aber nicht ausgeführt, solange Sie sie nicht explizit anschaltet. Bearbeiten Sie nun die Scan Configuration und klicken Sie auf das -Symbol vor *Nmap NSE*, um zur Liste der darin zusammengefassten NVTs zu gelangen. Über den ersten Eintrag (*Launch Nmap NSE Tests*) können Sie festlegen, ob NSE-Skript ausgeführt werden sollen. Klicken Sie auf das -Symbol bei diesem Eintrag um auf dessen Konfiguration zuzugreifen.




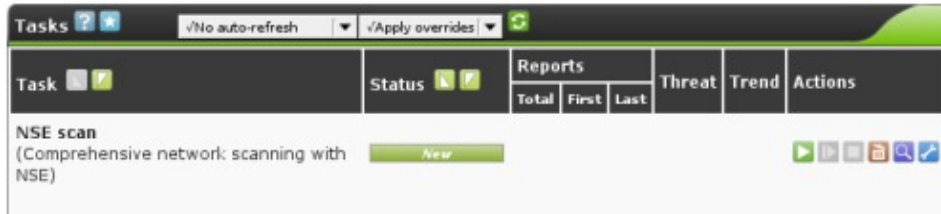
Setzen Sie den Parameter *Launch Nmap NSE Tests* auf "yes" und speichern Sie die Konfiguration.




## Ausführen des Scans

Nachdem Sie nun Ihre Scan Configuration vorbereitet haben, können Sie ein oder mehrere Ziele hinzufügen. NSE-Skripte können ohne Authentifizierung ausgeführt werden, Sie müssen also keine Zugangsdaten für die Ziele angeben.

Erstellen Sie nun den Task und starten Sie den Scan, indem Sie auf das -Symbol klicken.



Während des laufenden Scans können Sie die bereits vorliegenden Ergebnisse durch einen Klick auf das -Symbol einsehen und die Anzeige durch einen Klick auf das -Symbol aktualisieren.



Sobald der Status "Done" erreicht ist, liegen die kompletten Ergebnisse vor.




The screenshot displays four Nmap NSE (Nmap Scripting Engine) results, each with a severity level of 'Low'. The results are as follows:

- Low** (domain (53/tcp)): NVT: Nmap NSE: DNS Recursion (OID: 1.3.6.1.4.1.25623.1.0.801690). Result found by Nmap Security Scanner (dns-recursion.nse) http://nmap.org: dns-recursion: Recursion appears to be enabled.
- Low** (domain (53/tcp)): NVT: Nmap NSE: DNS Random Source Ports (OID: 1.3.6.1.4.1.25623.1.0.801688). Result found by Nmap Security Scanner (dns-random-srcport.nse) http://nmap.org: dns-random-srcport: 212.95.126.10 is POOR: 39 queries in 5.0 seconds from 1 ports with std dev 0.
- Low** (domain (53/tcp)): NVT: Nmap NSE: DNS Random TXID (OID: 1.3.6.1.4.1.25623.1.0.801689). Result found by Nmap Security Scanner (dns-random-txid.nse) http://nmap.org: dns-random-txid: 212.95.126.10 is GREAT: 40 queries in 5.2 seconds from 40 txids with std dev 18384.
- Low** (ftp (21/tcp)): NVT: Nmap NSE: Banner Grabber (OID: 1.3.6.1.4.1.25623.1.0.801253). Result found by Nmap Security Scanner (banner.nse) http://nmap.org: banner: 220 ProFTPD 1.2.10 Server (Debian) [192.168.46.27].

## Anpassung der Parameter

Einige Skripte können durch Parameter angepasst werden. Die Voreinstellungen sind eher zurückhaltend oder leer. Durch eine Anpassung der Parameter können Sie die Leistung und Genauigkeit des Scans verbessern.

Öffnen Sie noch einmal die Scan Configuration und importieren Sie die NSE-Scan Configuration ein zweites Mal. Dadurch erhalten Sie einen zweiten Eintrag, den Sie jetzt bearbeiten können. Klicken Sie nun auf das Symbol  vor der Scan Configuration, dann auf das Symbol vor der "Nmap NSE"-Kategorie. Nun können Sie die Parameter für die einzelnen Skripte anpassen. Einige Parameter erfordern Erfahrung und/oder eine genaue Kenntnis des Skripts für eine sinnvolle Anpassung. Weitere Informationen erhalten Sie über das [NSE reference portal](#) (englisch).

Die folgende Abbildung zeigt das Setzen eines solchen Parameters. Hier wird die SNMP Community gesetzt, um eine Systembeschreibung zu erhalten.

Edit Scan Config NVT Details ?

[Back to Config Family Details](#)

Config: NSE scanning  
Family: Nmap NSE

## Edit Network Vulnerability Test

### Details

**Name:** Nmap NSE: SNMP System Description  
**Summary:** Extract system information from an SNMP version 1 service  
**Family:** Nmap NSE  
**OID:** 1.3.6.1.4.1.25623.1.0.801801  
**CVE:**  
**Bugtraq ID:**  
**Other references:**  
**Tags:**  
**CVSS base:**  
**Risk factor:** None

### Description

**Overview:** This script attempts to extract system information from an SNMP version 1 service.

This is a wrapper on the Nmap Security Scanner's (<http://nmap.org>) snmp-sysdescr.nse.

### Preferences

Name	Value	Actions
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/> <input type="text"/>	
snmpcommunity :	<input type="text" value="corporate"/>	