

Task: Running Nmap scripts

Content

- [Execute simple network scanning with NSE](#)
- [Running the scan](#)
- [Parameter Tuning](#)

Introduction

Nmap is the most widely used de-facto standard tool of the security experts for network exploration. Nmap integrates a LUA scripting engine and dozens of scripts with various detection routines.

Greenbone Security Manager (GSM) integrates Nmap as core element for the phase of network exploration. For security experts the GSM also provides access to special abilities of Nmap such as the NSE scripts.


Greenbone Security Manager allows to run Nmap Scripting Engine (NSE) to extend the results of network exploration. This also allows to manage results of NSE scripts in the very same way as the other NVT's are managed, for example regarding annotation, severity overrides, filtering, reporting, etc.

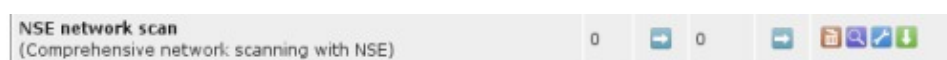
Execute simple network scanning with NSE

You can import [nmap-nse.xml](#) to quickly get a ready to run scan configuration. You can then skip the following phase and directly go to [Running the scan](#).





In the next step, we will create a new empty scan configuration and enable NSE manually to illustrate the whole process. Default configurations already include NSE but its execution is controlled by a global parameter which is off by default.

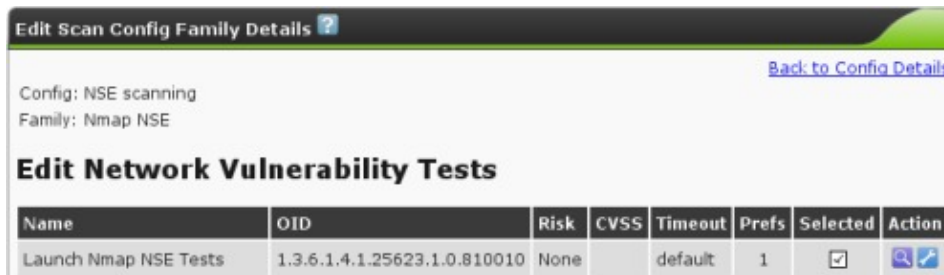
Click  to edit your configuration.



Select the *Nmap NSE* family to enable the execution of the NSE scripts for this configuration. Save the configuration.





NSE scripts are now considered for execution but won't run unless you explicitly turn them on. In your scan configuration panel, click the  icon in front of *Nmap NSE* to get the list of related NVTs. The first one, called *Launch Nmap NSE Tests*, is the one that controls the execution of the others. Click its  icon to access its configuration.

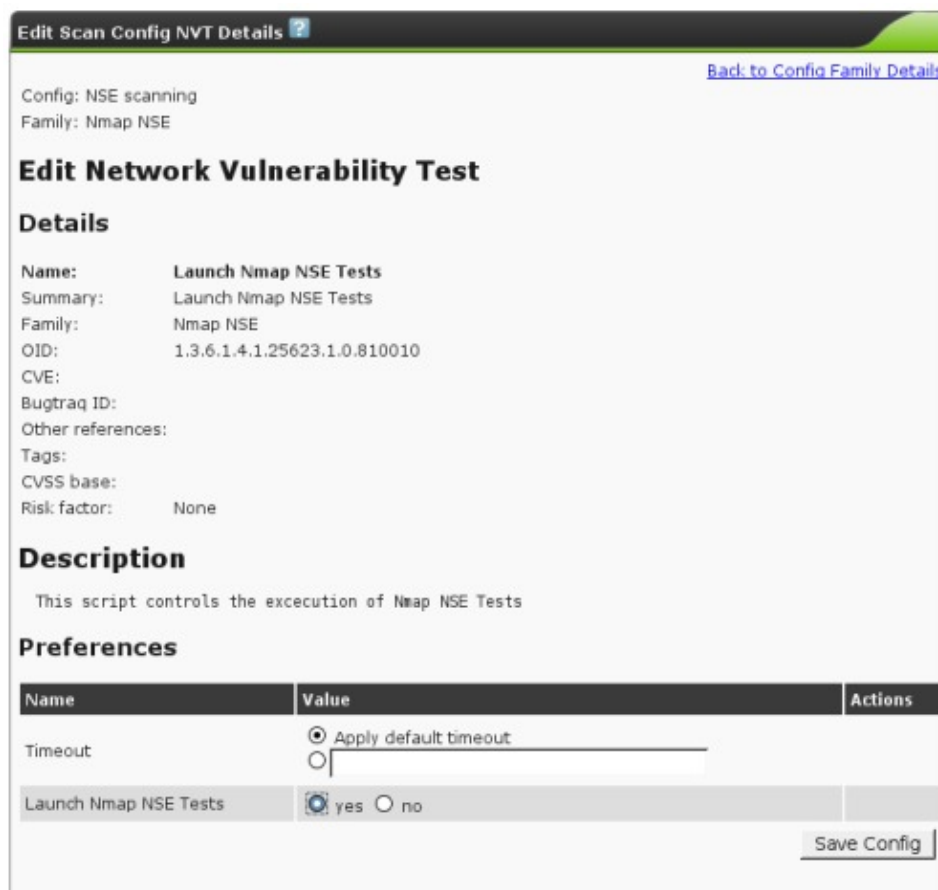


Config: NSE scanning
Family: Nmap NSE

Edit Network Vulnerability Tests

Name	OID	Risk	CVSS	Timeout	Prefs	Selected	Action
Launch Nmap NSE Tests	1.3.6.1.4.1.25623.1.0.810010	None		default	1	<input checked="" type="checkbox"/>	 

Set the *Launch Nmap NSE Tests* parameter to "yes" and save the configuration.



Config: NSE scanning
Family: Nmap NSE

Edit Network Vulnerability Test

Details

Name: Launch Nmap NSE Tests
Summary: Launch Nmap NSE Tests
Family: Nmap NSE
OID: 1.3.6.1.4.1.25623.1.0.810010
CVE:
Bugtraq ID:
Other references:
Tags:
CVSS base:
Risk factor: None

Description

This script controls the execution of Nmap NSE Tests

Preferences

Name	Value	Actions
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/> <input type="text"/>	
Launch Nmap NSE Tests	<input checked="" type="radio"/> yes <input type="radio"/> no	

Running the scan

Now that your scan configuration is ready, you can add the target(s). NSE scripts are non-authenticated checks. You don't need to supply credentials to execute them.

Then create the actual task, and start the scan by clicking .

You can check the results by clicking and refresh the display with at any time during the scan.

	High	Medium	Low	Log	Info	Total	Download
Full report:	0	0	64	77	0	141	PDF
All filtered results:	0	0	64	0	0	64	PDF
Filtered results 1 - 64:	0	0	64	0	0	64	PDF


When the status changes to "Done" the complete report is available.

- 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 16384
- 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]


Parameter tuning

Some NSE scripts can be tuned via parameters. The defaults are conservative or simply empty. It is possible to tune the scripts to increase the scan performance and accuracy.

Go back to the scan configuration page and import the NSE scan configuration again. You will have a second

entry you can edit now. Click the edit icon  in front of the scan configuration, then the one in front of the "Nmap NSE" category. You can then adjust the parameters for each script. Some parameters may need experience and/or deep understanding of the scripts to be chosen correctly. You can refer to the [NSE reference portal](#).

The following screenshot illustrates the setting of such a parameter. Here we supply the SNMP community string to use to gather system description.

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 style="width: 100%;" type="text"/>	
snmpcommunity :	<input style="width: 80%;" type="text" value="corporate"/>	