

4. Getting started: Performing an audit

Introduction

Security scans enable systems administrators to identify and assess possible risks within a network. Through GFI LANguard N.S.S. this is performed automatically, without all the unnecessary repetitive and time-consuming tasks related to performing them manually.

In this chapter you will discover how to perform security scans using default and custom settings, how to start scans directly from the toolbar and how to configure scan ranges.

To perform a security audit the scanning engine requires you to specify three primary parameters:

1. Target computer(s) to scan for security issues.
2. Scanning profile to use (specifies vulnerability checks/tests to be done against the specified targets).
3. Authentication details to be used to log on to the target computer(s).

For a thorough security scan use the *'Full Scan'* option.

About authentication credentials

When performing a security scan GFI LANguard N.S.S. must authenticate to the target computer(s) in order to execute the vulnerability checks and retrieve system information.

To achieve this, GFI LANguard N.S.S. must 'physically' log on to the target computer(s) with administrative rights i.e. using a local administrator account, domain administrator, enterprise administrator account or any other account that has administrative privileges over the target computer(s). Different systems often require different authentication methods. For example, to scan Linux systems you are often required to provide a private key file instead of the conventional password string.

NOTE 1: For more information about authentication methods refer to the 'Computer Profiles' section in the 'Configuring GFI LANguard N.S.S.' chapter.

NOTE 2: For more information about Public Key authentication, refer to the 'About SSH Private Key file authentication' section in the 'Configuring GFI LANguard N.S.S.' chapter.

About the scanning process

The target computer scanning process has three distinct stages.

Stage 1: Determine availability of target computer:

During this stage, GFI LANguard N.S.S. will determine whether a target computer is available for vulnerability scanning. This is

achieved through connection requests that are sent in the form of NETBIOS queries, SNMP queries and/or ICMP pings.

NOTE: By default, GFI LANguard N.S.S. will NOT scan the devices that fail to respond to the connection requests sent via NETBIOS queries/SNMP queries/ICMP pings.

Stage 2: Establish connection with target device:

In the second stage of its target scanning process, GFI LANguard N.S.S. will establish a direct connection with the target computer by remotely logon on to it. This is achieved using the scan credentials configured in step 5 of the new scan wizard.

Stage 3: Execute vulnerability checks:

During this final stage, GFI LANguard N.S.S. will execute the vulnerability checks configured within the selected scanning profile. This will result in the identification and reporting of specific weaknesses present on your target computer.

NOTE 1: GFI LANguard N.S.S. ships with a default list of scanning profiles that are preconfigured with vulnerability checks. Nevertheless you can also customize both the scanning profiles and the vulnerability checks contained within. For more information on how to achieve this refer to the “Scanning Profiles’ chapter.

NOTE 2: Please note that if any type of Intrusion Detection Software (IDS) is running during scans, GFI LANguard N.S.S. will set off a multitude of IDS warnings and intrusion alerts in these applications. If you are not responsible for the IDS system, make sure to inform the person in charge about any planned security scans.

NOTE 3: Along with the IDS software warnings, kindly note that a lot of the scans will show up in log files across diverse systems. UNIX logs, web servers, etc. will all show the intrusion attempts made by the computer running GFI LANguard N.S.S. If you are not the sole administrator at your site make sure that the other administrators are aware of the scans you are about to run.

Performing a security scan using default settings

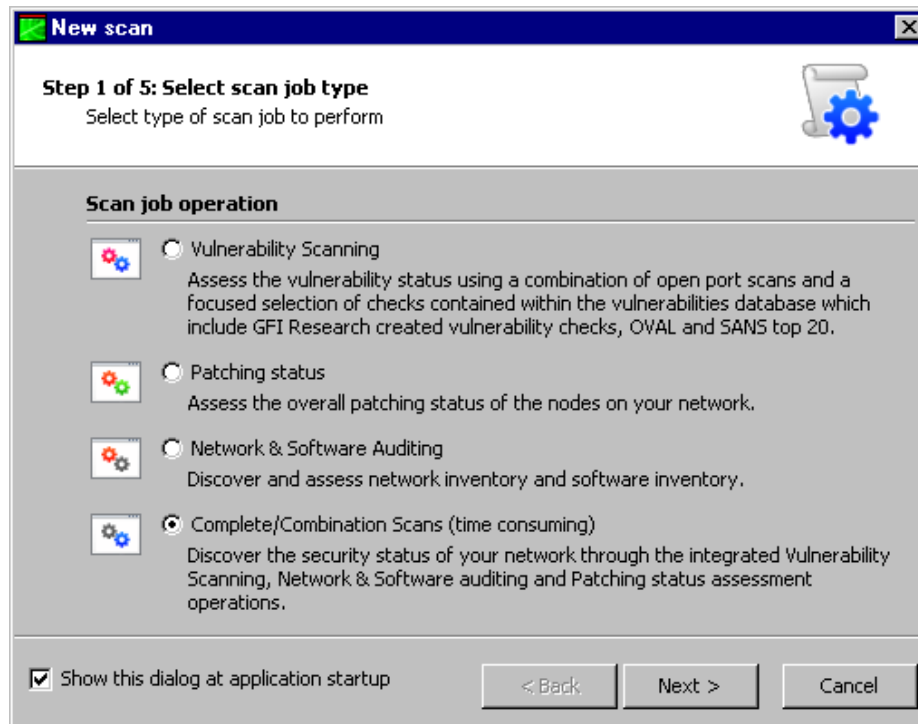
Out of the box, GFI LANguard N.S.S. includes default configuration settings that allow you to run immediate scans soon after the installation is complete.

For a default scan you must only specify which target computer(s) you wish to audit and GFI LANguard N.S.S. will automatically:

- Authenticate to the targets using the currently logged on user account credentials (i.e. the credentials under which GFI LANguard N.S.S. is currently running).
- Use a thorough list of default vulnerability checks that are preconfigured in the ‘Full’ scanning profile. This is one of the default scanning profiles that ships with GFI LANguard N.S.S.

To perform your first scan, do as follows:

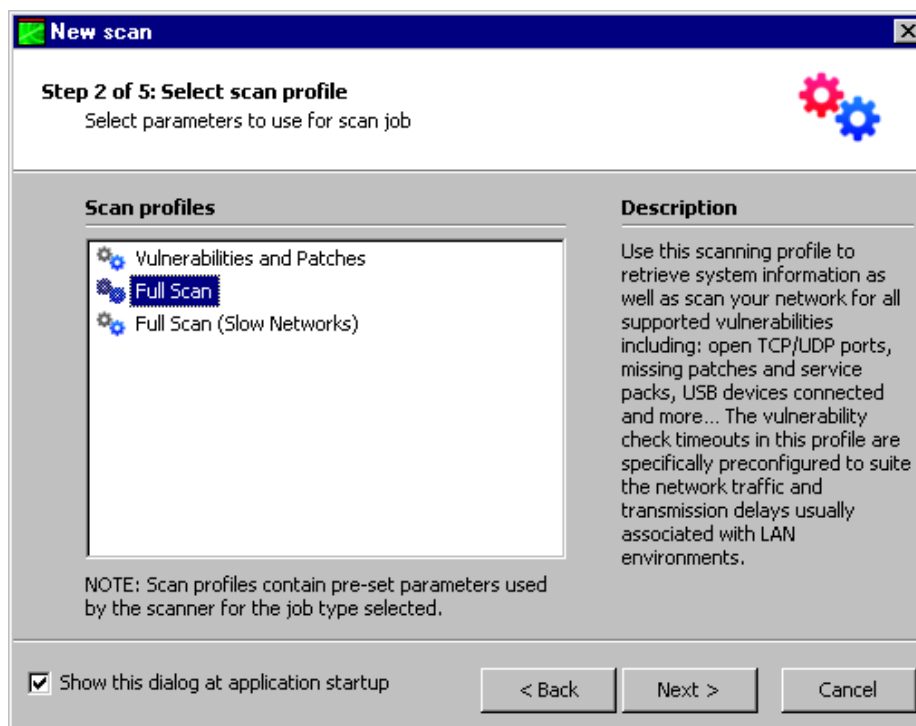
1. Click on **New Scan...** button



Screenshot 12 - Selecting the type of security scan

2. Select one of the following scanning operations and click **Next**:

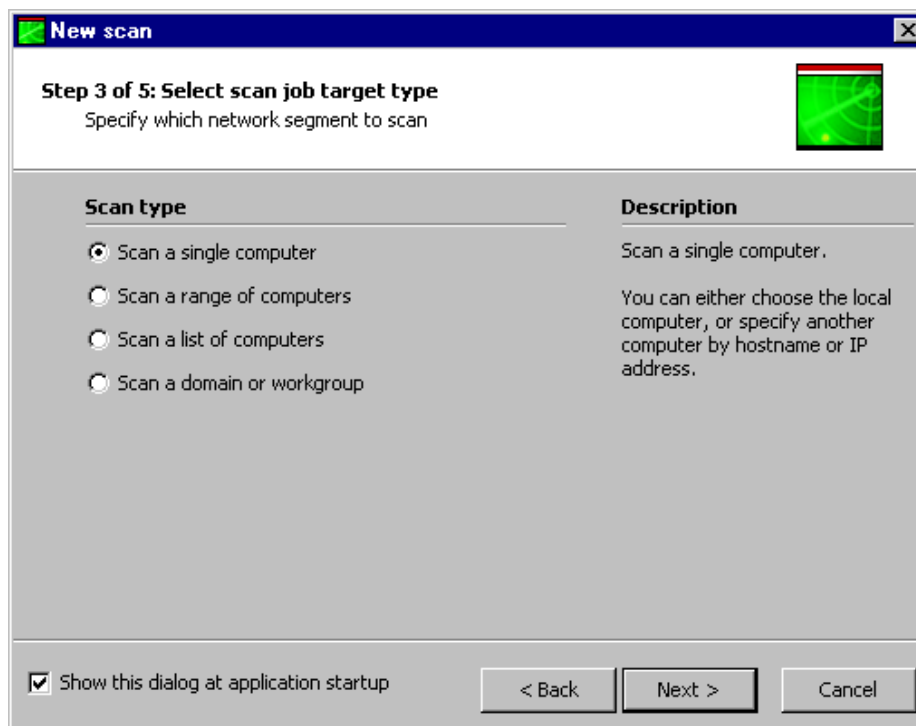
- *'Vulnerability Scanning'* – Use this scanning operation to enumerate all the vulnerabilities present on target computers including missing patches.
- *'Patching status'* – Use this scanning operation to enumerate only missing patches on target computers.
- *'Network and Software Auditing'* – Use this scanning operation to enumerate system information without including vulnerabilities and missing patches.
- *'Complete/Combination scan'* – Use this scanning operation to retrieve system information and enumerate all vulnerabilities including missing patches.



Screenshot 13 - Choose the scanning profile

3. Select the required scanning profile and click **Next**.

NOTE: For a detailed description of what each individual scanning profile does please refer to the “*Scanning profile description*” section in the Scanning Profiles chapter in this document.

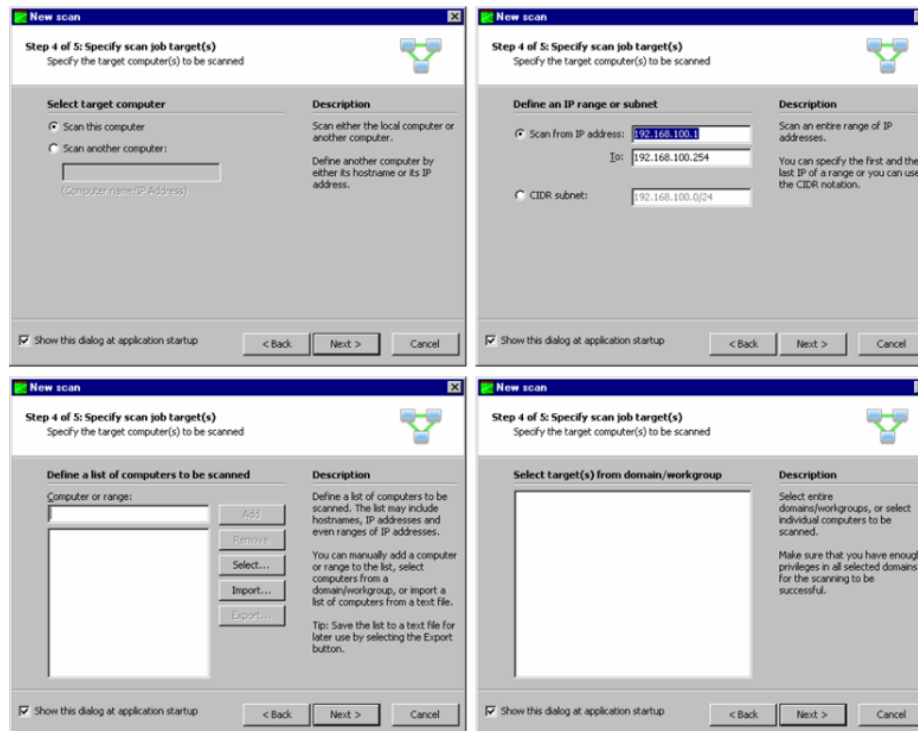


Screenshot 14 - Selecting scan range

4. Select one of the following scan target types and click **Next**:

- ‘*Scan single computer...*’ – Select this option to scan a single computer.

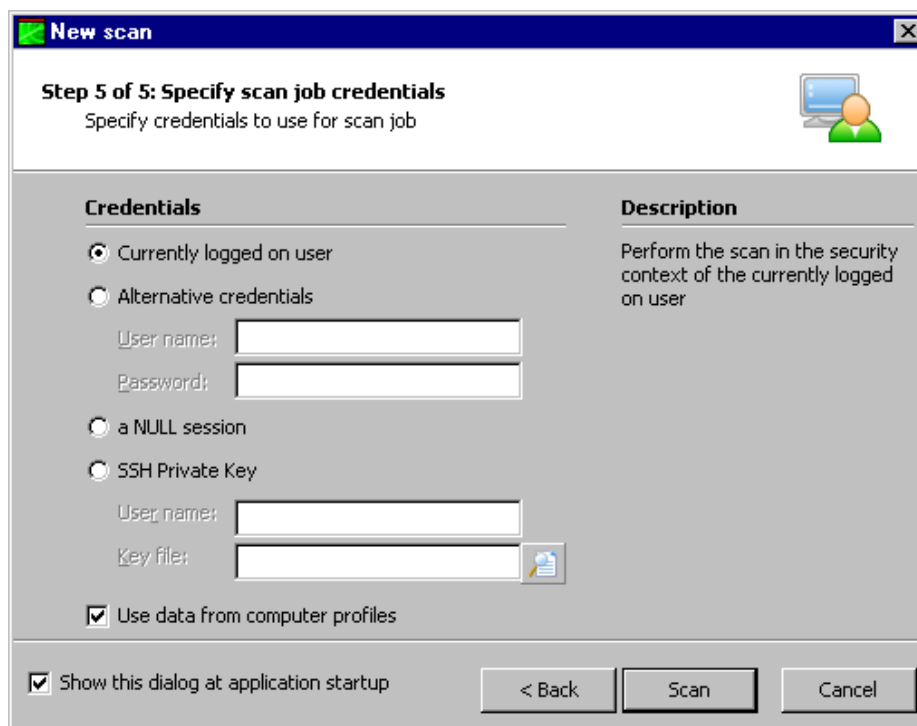
- ‘Scan range of Computers...’ – Select this option to scan a specific range of computers.
- ‘Scan list of Computers...’ – Select this option to scan a custom list of computers.
- ‘Scan a Domain...’ – Select this option to scan an entire Windows domain.



Screenshot 15 - New Scan range options dialogs.

5. Specify scan target details (i.e. host name, IP, range of IPs or domain name) and click **Next**.

NOTE: When configuring IP ranges, GFI LANguard N.S.S. 8.0 also allows you to specify which IPs must be excluded from this range. For more information on this feature please refer to **Configuring scan ranges** section in this document.

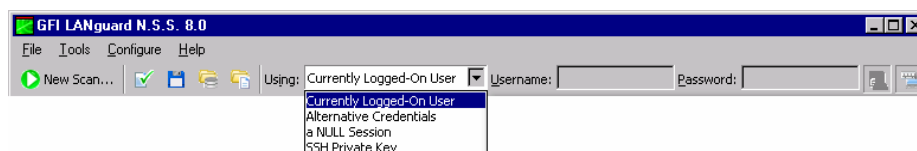


Screenshot 16 - Specify the scan credentials

6. Specify the authentication details to be used during this scan. Click on the **Scan** button to initiate the scanning process.

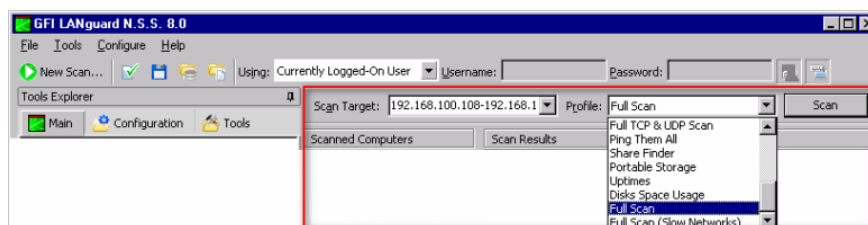
Quick-start scans using currently logged on user credentials

You can trigger network vulnerability scans directly from the toolbar without having to perform major configurations as well as without bringing up the new scan wizard. To achieve this:



Screenshot 17 - GFI LANguard N.S.S. new scan toolbar

1. From credentials drop-down list provided in the toolbar select the **Currently logged on user** option.



Screenshot 18 - GFI LANguard N.S.S. target details toolbar

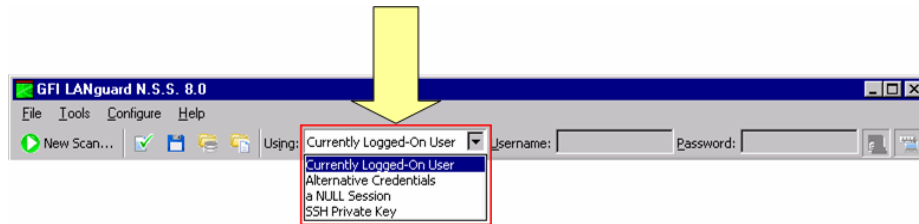
2. In 'Scan Target' drop down, specify the targets to be scanned using these credentials (for example, TMJason, 130.12.1.20-130.12.1.30, etc.).

3. From the 'Profile' drop down select the scanning profile to be used for this network vulnerability scan.

4. Click on **Scan** to initiate the scanning process.

Quick-start scans using alternative logon credentials

To run a network security audit using alternative logon credentials:

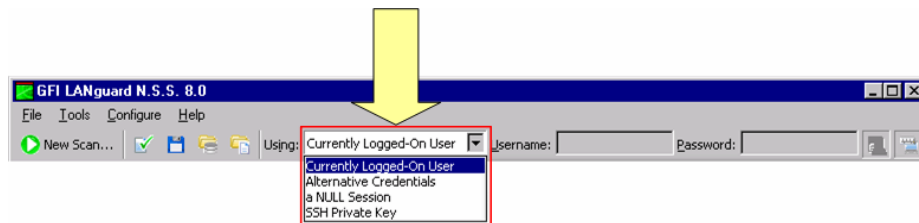


Screenshot 19 - GFI LANguard N.S.S. new scan toolbar: Authentication methods drop down list

1. From credentials drop-down list provided in the toolbar select the **Alternative credentials** option.
2. In the adjacent fields specify the username and password to be used during this scan.
3. Configure the rest of the options as described in the 'Quick-start scans using currently logged on user credentials' section above.

Quick start scans using SSH Private Key

To run a network security audit using SSH Private key credentials do as follows:



Screenshot 20 - GFI LANguard N.S.S. new scan toolbar: Authentication methods drop down list

1. From credentials drop-down list provided in the toolbar select the **SSH Private key** option.
2. In the adjacent fields specify the username and private key file to be used during this scan.
3. Configure the rest of the options as described in the 'Quick-start scans using alternative credentials' section above.

Quick-start scans using a null session

One of the most serious threats in a network system is the misconfiguration of passwords. Default passwords or even worse blank password (technically referred to as 'null' passwords) are a big vulnerability because they could easily allow malicious users to gain access to your system without any considerable effort. GFI LANguard N.S.S. allows you to specifically verify whether your target computers have null passwords through a 'null session'. During null sessions, the scanning engine will attempt to logon to a target computer with blank credentials. The benefit of such an exercise is that if such a scan is successful, it means your target is accessible without the need of logon credentials. To run a null session:

1. From credentials drop-down list provided in the toolbar select the **Null Settings** option.
2. In 'Scan Target' drop down, specify the targets to be scanned during this null session.
3. From the 'Profile' drop down select the scanning profile to be used during this network vulnerability scan.
4. Click on **Scan** to initiate the scanning process.