Performing a Security Assessment

Security Assessment Overview

The Security Assessment Module allows you to deliver IT security assessment services to your client – even if you aren't an IT security expert. Just run the installation-free scanning tool, import the scan results into our proprietary risk analyzer, customize the reports with your own company name and branding elements, and run the reports. The Security Assessment Module has many uses for your MSP, including:

- Generate executive-level reports that include a proprietary Security Risk Score and Data Breach Liability Report along with summary charts, graphs and an explanation of the risks found in the security scans.
- Identify network "share" permissions by user and computer. Provide comprehensive lists of all network shares, detailing which users and groups have access to which devices and files, and what level of access they have.
- Catalog external vulnerabilities including security holes, warnings, and informational items that can help you make better network security decisions, plus a full NMap Scan which checks all 65,535 ports and reports which are open. This is an essential item for many standard security compliance reports.
- Methodically analyze login history from the security event logs. The report uses mathematical modeling and proprietary pattern recognition to highlight potential unauthorized users who log into machines they normally do not access and at times they normally do not log in.

What You Will Need

<table>
<thead>
<tr>
<th>Security Assessment Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Detective</td>
<td>The Network Detective Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.</td>
</tr>
<tr>
<td>Security Assessment Component</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Security Assessment Data Collector</strong></td>
<td>The Network Detective Security Assessment Data Collector (SADC) is a windows application that performs the data collections for the Security Assessment Module.</td>
</tr>
<tr>
<td><strong>Push Deploy Tool</strong></td>
<td>The Network Detective Push-Deploy Tool pushes the local data collector to machines in a specified range and saves the scan files to a specified directory (which can also be a network share). The benefit of the tool is that a local scan can be run simultaneously on each computer from a centralized location.</td>
</tr>
</tbody>
</table>
Network Prerequisites for Network Detective Scans

For a successful network scan:

1. **Ensure all network endpoints are turned on throughout the duration of the scan.** This includes PCs and servers. The scan can last several hours.

2. **Configure the target network to allow for successful scans on all network endpoints.** See [Pre-Scan Network Configuration Checklist](#) for configuration guidance for both Windows Active Directory and Workgroup environments.

3. **Gather the information below to configure your scans for the client site.** Work with the project Technician and/or your IT admin on site to collect the following:
   - **Admin network credentials** that have rights to use WMI, ADMIN$, and File and Printer Sharing on the target network.
   - **Internal IP range** information to be used when performing internal scans.

   **Note:** Network Detective will automatically suggest an IP range to scan on the network. However, you may wish to override this or exclude certain IP addresses.

   - **External IP addresses** for the organisation to be used when setting up External Vulnerability Scans.
   - **Network Detective User Credentials**
     - For Windows Active Directory environments, you will need admin credentials to connect to the Domain Controller, as well as the name/IP address of the domain controller.
     - For Windows Workgroup network environments, a list of the Computers to be included in the Assessment and the Local Admin Credentials for each computer.
Follow these steps to perform a Security Assessment.

Step 1 — Download and Install the Network Detective Application

Go to www.rapidfiretools.com/nd to download and install the Network Detective application on a PC on the MSP network. Then run Network Detective and log in with your credentials.

Step 2 — Create a New Site

To create a new site:

1. Open the Network Detective Application and log in with your credentials.
2. Click **New Site** to create a new Site for your assessment project.
3. Enter a **Site Name** and click **OK**.
Step 3 — Start a Security Assessment

1. From within the Site Window, select the Start button that is located on the far right side of the window to start the Assessment.

   ![Start button](Image)

   Next, select the Security Assessment option presented.

   ![Select Assessment Type](Image)

   Then follow the prompts presented in the Network Detective Wizard to start the new Assessment.

2. Once the new Security Assessment is started, a “Checklist” is displayed in the Assessment Window presenting the “Required” and “Optional” steps that are to be performed during the assessment process. Below is the Checklist for a Security Assessment.

   ![Assessment Window](Image)

3. Complete the required Checklist Items and use the Refresh Checklist feature to guide you through the assessment process at each step until completion.

   You may also print a copy of the Checklist for reference purposes by using the
Printed Checklist feature.

Step 4 — Initiate External Vulnerability Scan

Select Initiate External Scan button to start an External Vulnerability Scan.

Enter the range of IP addresses you would like to scan. You may enter up to 16 external addresses.
Select Add to add a range of external IP addresses to the scan. If you do not know the external range, you can use websites such as whatismyip.com to determine the external IP address of a customer.

![Add IP Address Range](image1)

Enter the IP range for the scan. For just one address, enter the same value for the Starting and Ending IP Address.

You can initiate the External Vulnerability Scan before visiting the client’s site to perform the data collection. This way, the External Scan data should be available when you are ready to generate the client’s reports.

![Initiate External Vulnerability Scan](image2)

In the Initiate External Vulnerability Scan window, enter an email address to be notified when the scan is completed.

Click Next to send the request to the servers that will perform the scan.
Scans can take several hours to complete. You will receive an e-mail when the External Vulnerability Scan is complete.

Next, select the **Refresh Checklist** option to update the status of the **External Vulnerability Scan** that is listed under the **Scans** bar.

The **Assessment Window** and associated **Scans** listed under the **Scans** bar at the bottom of the **Assessment Window** will be updated to reflect the External Vulnerability Scan has been initiated and its completion is pending.

Refer to the **Scans** list within the **Assessment Window** detailed in the figure below.

The scan’s pending status of “0 of 1 complete” will be updated to **Completed** once the scan is completed. An email message stating that “the scan is complete” will also be sent to the person’s email address that was specified when the scan was set up to be performed.

Upon the scan’s completion, note that the **External Vulnerability Scan** with its **Completed** status will be listed as an imported scan under the **Scans** bar at the bottom of the **Assessment Window** as presented below.

---

**Step 5 — Perform Security Scan Data Collection**

Download and run the Network Detective Data Collector on a PC on the target network. Use the Data Collector to scan the target network.

2. Run the **Security Data Collector** executable program as an Administrator (**right click**>**Run as administrator**).

3. **Unzip** the files into a temporary location. The Security Data Collector’s self-extracting ZIP file does not install itself on the client computer.

4. The Security Data Collector Scan Type window will appear.

   Select the **Security Data Collector** and **Perform Network Scan** options. Click **Next**.

5. The **Active Directory** window will appear. Select the type of network you are scanning (**Active Directory domain** or **Workgroup**).
Next enter the required administrative credentials to access the network during the scan.

- If in a domain, enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory. Click Next to test a connection to the local Domain Controller and Active Directory to verify your credentials.
- If you are scanning a Workgroup environment, select Workgroup, click OK, and skip to #7.

6. The Local Domains window will appear. Select the Domains to scan. Choose whether to scan all domains or only specific domains and OUs. Click Next.

Note: If you select to scan a Workgroup, the Security Data Collector will skip this step.
Confirm your selections if you opt to scan only specific Domains and OUs. Click OK.

7. The **Additional Credentials** screen will appear. Enter any additional credentials to be used during the scan. Click **Next**.

**Note:** If you selected Workgroup on the Active Directory window, enter credentials which can access the individual workstations as a local administrator.
8. The **IP Ranges** screen will then appear. The Security Data Collector will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.

From this screen you can also:
• Click **Reset to Default** to reset to the automatically suggested IP Range.

• Click **Import from Text File** to import a predefined list or range of IP addresses.

**Important:** Scans may affect network performance. Select **Perform minimal impact scan** if this is an issue.

When you have entered all IP Ranges to scan, click **Next**.

**Important:** If you are scanning a large number of IP addresses, confirm that you wish to continue. Consider performing multiple scans on smaller IP ranges. You can then upload each "batch" of scan files into the assessment, where they will be merged for complete results.

9. The **User Control Tests** screen will appear. These tests will attempt to access sites in various categories from this computer. This can help determine how much access a user has to potentially risky websites. You can choose to opt out of the tests by deselecting categories. You can also enter your own custom URLs and categories to test. Then click **Next**.
10. The **File Scanner** screen will appear. Choose whether to scan for PII (Personally Identifiable Information) and click **Next**.

11. The **Verify and Run** window will appear. Select the folder that you want to store the scan data file in after the scan is completed. You may also change the scan’s **Output Assessment File Folder** location and **Basename** for the scan data. The file will be output as a *.SDF* file.
Tip: Use the Pre-scan Analyzer to identify and correct any configuration issues prior to running the Network Scan. The Push Deploy tab will indicate which assets are fully accessible for scanning to ensure a more thorough scan. Pre-scan results and recommendations are provided at the completion of the pre-scan.

Enter any Comments and then click Start.

12. The Collection Progress window will appear. The Network Scan’s status is detailed in the Collection Progress window. The Collection Progress window presents the progress status of a number of scanning processes that are undertaken.
At any time you can **Cancel Data Collection** which will not save any data. By selecting **Wrap It Up** you can terminate the scan and generate reports using the incomplete data collected.

Upon the completion of the scan, the **Finish** window will appear. The **Finish** window indicates that the scan is complete and enables you to review the scan output file’s location and the scan’s **Results Summary**.
Click **Done** to close the **Security Data Collector** window. Note the location where the scan’s output file is stored.

**Step 6 — Use the Push Deploy Tool**

Download and run the Push Deploy Tool on a PC on the target network. Use it to perform local data scans on all computers.

1. Visit the RapidFire Tools software download website at [https://www.rapidfiretools.com/nd](https://www.rapidfiretools.com/nd) and download the Push Deploy Tool.

2. **Unzip** the files onto a USB drive or directly onto any machine on the target network.

3. From within the unzipped folder, run the **NetworkDetectivePushDeployTool.exe** executable program as an Administrator (**right click>Run as administrator**).
Important: You must run the Push Deploy Tool as an Administrator.

The Push Deploy Tool Settings and Configuration window will appear.

4. Set the **Storage Folder location** and select the **Security Scan** option.

**Tip:** For your convenience, create a shared network folder to centralize and store all scan results data files created by the Push Deploy Tool. Then reference this folder in the **Storage Folder** field to enable the local computer scan data files to be stored in this central location.

If additional credentials are required, type in the administrator level **Username** and **Password** necessary to access the local computers on the network to be scanned. Then click **Add**.
Important: For the **Push Deploy Tool** to push local scans to computers throughout the network, ensure that the following prerequisites are met:

- **Ensure that the Windows Management Instrumentation (WMI) service is running** and able to be managed remotely on the computers that you wish to scan. Sometimes Windows Firewall blocks Remote Management of WMI, so this service may need to be allowed to operate through the Firewall.

- **Admin$ must be present on the computers you wish to scan**, and be accessible with the login credentials you provide for the scan. Push/Deploy relies on using the Admin$ share to copy and run the data collector locally.

- **File and printer sharing must be enabled** on the computers you wish to scan.

- **For Workgroup based networks, the Administrator credentials for all workstations and servers that are to be scanned are recommended to be the same.** In cases where a Workgroup-based network does not have a one set of Administrator credentials for all machines to be scanned, use the Add option to add all of the Administrator credentials for the Workgroup. Multiple sets of Administrator credentials will be listed in the Credentials box.

5. Click **Next** after you have configured the Push Deploy Tool.
6. The **Computers and Status** window will appear. From here you can:
   - **Add a Single Computer** to be scanned
   - **Add (computers) from File** that are to be scanned
   - **Add (computers) from IP Range** that are to be scanned
   - **Or Save Computers to File** in order to export a list of computers to be
7. When you have input the IP address range into the IP Range window, select the OK button.

After one or more of the above-mentioned methods have been used to define the computer IP addresses to be scanned, the computer names and IP addresses will be listed in the Computers and Status window.

8. Start the scan either by selecting the “unpause” button in the Computer and Status window, or, by selecting the Next button in the Computer and Status window and the scan will be initiated. The status of each computer’s scan activity will be highlighted within the Computers and Status window as presented below.
Upon the completion of all of the scheduled scans, the scan data collected is stored within the **Storage Location** folder presented in the **Collected Data Files** window of the **Push Deploy Tool**.

9. To verify the inclusion of the scan data produced by the **Push Deploy Tool** within your assessment, select the **Next** button within the **Push Deploy Tool**. The **Collected Data Files** window will be displayed.

![Collected Data Files Window](image)

10. To review or access the files produced by the **Push Deploy Tool**’s scans, select the **On Finish: Open Storage Folder** option in the **Collected Data Files** window. Then click **Finish**.

MORE INFO:
The Push Deploy Tool pushes the local data collector to machines in a specified range and saves the scan files to a specified directory (which can also be a network share). The benefit of the tool is that a local scan can be run simultaneously on each computer from a centralized location.

The output files (.ZIP, files) from the local scans can be stored on a USB drive and taken off site to be imported into the active assessment within Network Detective.

After all of the **Security Scans** are complete, the next phase in the process is to import the scan data files produced by the **Security Scan** into the current assessment.
Step 7 — Import Scans into Network Detective App

Make sure you can access all of the scan data files from the PC on the MSP network where you have Network Detective installed. Then, import the data collected by the Data Collector into the Security Assessment.

1. Click **Import Scan File** on the **Scans** bar in the Network Detective **Assessment** window.

![Import Scan File](image)

The **Select the Scan Results** window will be displayed.

![Select the Scan Results](image)

2. Click **Browse** in the **Scan Results** window and select all data file(s) that you wish to import.

3. For a Security Scan, these will be:
• .cdf file for the computer scans
• .sdf file for the security data scans
• .ndf file for the network scans

4. Click **Open** button to import the scan data. Then click **Next**.

5. An archived copy of the scan will be created in the Network data directory. You can access this at `%APPDATA%\NetworkDetective` on your PC. Click **Finish**.

   i. *If prompted*, use the **Network Detective Merger** to merge the data file(s) into the assessment. Select the Domain into which the file will be merged. Click **Merge Now**.

   ![Network Detective Merger](image)

   *The Scans bar will be updated with the imported scan files.*

Once all of the scan data is imported into the **Assessment**, the assessment’s **Checklist** will indicate that the **Reports** are ready to be generated.

![Reports Ready](image)
Step 8 — Generate Security Assessment Reports

Note: This step is NOT performed at the client site or network. Network Detective should be installed on your workstations or laptop. Install Network Detective from www.rapidfiretools.com/download if you have not already done so. To generate the reports for your Security Assessment, follow the steps below:

1. Run Network Detective and log in with your credentials.
2. Then select the Site, go to the Active Assessment, and then select the Reports link to the center of the Assessment Window in order select the reports you want to generate.

3. Select the Create Reports button and follow the prompts to generate the reports you selected.
4. At the end of the report generation process, the generated reports will be made available for you to open and review.
Security Assessment Reports

The **Security Assessment** module can generate the following reports:

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomalous Login Report</td>
<td>The Anomalous Login Report shows suspicious logins by user and computer based on various probability criteria. The includes: A) logins into specific computers users don't normally log into, and B) logins by users outside of their regular pattern (not only by day of week, but also by time of day).</td>
</tr>
<tr>
<td>Consolidated Security Report Card</td>
<td>The Computer Security Report Card assesses individual computers at a high level based on various security criteria. Devices discovered on the network are assigned an overall score, as well as a specific score for each of the assessment categories detailed below. The scores are represented as color-coded letter grades ('A' through 'F'). The report card should be viewed as a relative measure as to how well a computer complies with security best practices. There may be specific reasons or compensating controls that may make it unnecessary to achieve an &quot;A&quot; in all categories to be considered secure.</td>
</tr>
<tr>
<td>Cyber Liability and Data Breach Report</td>
<td>Identifies specific and detailed instances of personal identifiable information (PII) and cardholder data throughout a computer network that could be the target of hackers and malicious insiders. It also calculates the potential monetary liability and exposure based upon industry published research.</td>
</tr>
<tr>
<td>Data Breach Liability Report</td>
<td>Small and midsize businesses need to manage their exposure to the financial risk that accompanies cyber threats. Data breaches come in many shapes and sizes. The average person hears &quot;data breach&quot; and probably thinks of hackers. But there are many kinds of cyber incidents, and most don't come from malware or ransomware. Instead they are the result of insider data breaches, data theft by employees, and employee mistakes. A breach is an event in which an individual's name plus a medical, financial, debit/credit card and other personal or sensitive information is potentially put at risk in electronic form. A compromised record is one that has been lost or stolen as a result of a data breach. The report not only identifies specific and detailed instances of personal identifiable information (PII) throughout your computer network that could be the target of hackers and malicious insiders but also calculates</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>the potential monetary liability based upon industry published research.</td>
<td></td>
</tr>
<tr>
<td><strong>External Network Vulnerabilities Summary Report</strong></td>
<td>This report provides a priority ordered listing of issues by their CVSS to enable technicians to prioritize the issues they are working on. This report provides an extremely compact view of all issues to provide a quick survey of the various issues that were detected in an environment.</td>
</tr>
<tr>
<td><strong>External Vulnerabilities Scan Detail Report</strong></td>
<td>A comprehensive output including security holes and warnings, informational items that can help make better network security decisions, plus a full NMap Scan which checks all 65,535 ports and reports which are open. This is an essential item for many standard security compliance reports.</td>
</tr>
<tr>
<td><strong>External Vulnerability Scan Detail by Issue Report</strong></td>
<td>A more compact version of the External Vulnerability Scan Detail report that is organized by issues. Devices that are affected are listed within an issue type. This report is useful for technicians that are looking to resolve specific issues identified within the environment, rather than performing remediation on a particular system.</td>
</tr>
<tr>
<td><strong>External Vulnerability Scan Detail in Excel Format</strong></td>
<td>An Excel version of the External Vulnerability Scan Detail report listing issues by device.</td>
</tr>
<tr>
<td><strong>Login Failures by Computer Report</strong></td>
<td>This report identifies users who have succeeded in logging in to another machine. This report is great for auditing/logging purposes to know of all login attempts.</td>
</tr>
<tr>
<td><strong>Login History by Computer Report</strong></td>
<td>Same data as User Behavior but inverted to show you by computer. Quite useful, in particular, for looking at a commonly accessed machines (file server, domain controller, etc.) – or a particularly sensitive machine for failed login attempts. An example would be CEO’s laptop – or the accounting computer where you want to be extra diligent in checking for users trying to get in.</td>
</tr>
<tr>
<td><strong>Outbound Security Report</strong></td>
<td>Highlights deviation from industry standards compared to outbound port and protocol accessibility, lists available wireless networks as part of a wireless security survey, and provides information on Internet content accessibility.</td>
</tr>
</tbody>
</table>
| **Resulting Set of Policies** | This report analyzes the various Resulting Sets of Policy (RSOP) based
<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>on user settings on computers in the environment and helps point out commonalities in the sets and which users/computer combinations have the configurations applied. There are separate reports for both user settings and computer settings.</td>
</tr>
<tr>
<td>Security Assessment PowerPoint</td>
<td>Use our generated PowerPoint presentation as a basis for conducting a meeting presenting your findings from the Network Detective. General summary information along with the risk and issue score are presented along with specific issue recommendations and next steps.</td>
</tr>
<tr>
<td>Security Management Plan</td>
<td>Network Management Plan This report will help prioritize issues based on the issue's risk score. A listing of all security related risks are provided along with recommended actions.</td>
</tr>
<tr>
<td>Security Policy Assessment Report</td>
<td>A detailed overview of the security policies which are in place on both a domain wide and local machine basis.</td>
</tr>
<tr>
<td>Security Risk Report</td>
<td>This report includes a proprietary Security Risk Score and chart showing the relative health (on a scale of 1 to 10) of the network security, along with a summary of the number of computers with issues. This powerful lead generation and sales development tool also reports on outbound protocols, System Control protocols, User Access Controls, as well as an external vulnerabilities summary list.</td>
</tr>
<tr>
<td>Share Permission Report</td>
<td>Comprehensive lists of all network “shares” by computer, detailing which users and groups have access to which devices and files, and what level of access they have.</td>
</tr>
<tr>
<td>Share Permission Report by User</td>
<td>Comprehensive lists of all network &quot;shares&quot; by user. Each subsection details the share and file system permissions granted to each user account within the above domain.</td>
</tr>
<tr>
<td>User Behavior Analysis Report</td>
<td>Shows all logins, successful and failure, by user. Report allows you to find service accounts which are not properly configured (and thus failing to login) as well as users who may be attempting (and possibly succeeding) in accessing resources (computers) which they should not be.</td>
</tr>
<tr>
<td>User Permissions</td>
<td>Organizes permissions by user, showing all shared computers and files to which they have access.</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Report</td>
<td></td>
</tr>
</tbody>
</table>