

# **UPGRADE GUIDE**

Migrate Inspector 2.0 to VulScan by RapidFire Tools

5/31/2022 1:11 PM

## Contents

VulScan Integration with Network Detective	3
Migrate Inspector 2 to VulScan	3
Log in to RapidFire Tools Portal and Access VulScan Site	5
Next Steps for New VulScan Users	6
Generate Internal Vulnerability Reports in Network Detective using VulScan	6
VulScan and Reporter	7

#### **RapidFireTools**\*

## VulScan Integration with Network Detective

### Migrate Inspector 2 to VulScan

Tip: You can find a video tutorial for upgrading to VulScan here.

As of Monday, January 26, 2021, **Inspector 2** will be deprecated and replaced by **VulScan**.

- Inspector 2 users will no longer have the ability to configure scan tasks using Network Detective.
- Instead, users must manage scans and review scan data using the VulScan console in the RapidFire Tools Portal.
- Inspector 2 users will have the benefits of the new VulScan product, and be able to download data into Network Detective to generate Internal Vulnerability Reports. (See <u>"Generate Internal Vulnerability Reports in Network Detective using VulScan"</u> <u>on page 6</u>.)

Inspector 2 users should follow these steps to upgrade to VulScan.

**Note:** To migrate your site, you must have the latest version of Network Detective: version 4.0.1299 or higher.

- 1. Open Network Detective and log in to your account.
- 2. Click the Help menu and select Migrate to Vulnerability Scanner.



3. Review the prompt and click OK.

Migratio	n to Vulnerability Scanner	×			
This is a one-time process to migrate existing Inspector 2 sites to Vulnerability Scanner sites that can be accessed and managed in the RapidFire Tools portal. If a site with an equivalent name already exists in the RapidFire Tools portal and is being used for Cyber Hawk or Compliance Manager, a new site will be created with the suffix -VS (i.e., "My Site" would turn into "My Site-VS"). Press OK to proceed with the site migration?					
	OK Cancel				

**Note:** This is a one-time process to migrate existing Inspector 2 sites to VulScan sites that can be accessed and managed in the RapidFire Tools portal.

**Important:** If a site with an equivalent name already exists in the RapidFire Tools portal and is being used for Cyber Hawk or Compliance Manager, a new site will be created with the suffix -VS (i.e., "My Site" would turn into "My Site-VS"). If you had a Reporter assigned to this site, you will need to manually move the Connector to the new site ("My Site-VS").

#### **RapidFireTools**\*

- 4. All of your existing Inspector 2 sites will be migrated to VulScan sites in the RapidFire Tools Portal.
- 5. The **Queued Scan Tasks** for your Inspector 2 sites will be carried over as scan tasks that can be managed from your VulScan site in the RapidFire Tools Portal. **UNSCHEDULED SCAN TASKS IN THE TASK LIBRARY WILL NOT BE MIGRATED.**

### Log in to RapidFire Tools Portal and Access VulScan Site

1. Once you migrate your site, access the RapidFire Tools Portal at <a href="https://www.youritportal.com">https://www.youritportal.com</a> and log in with your credentials.

RapidFireTools
Welcome Back
Username
Remember me on this computer
Forgot Password? Log in

2. Select your new site from the Site page. You can then begin using VulScan.

RapidFire Tools! Site	To Do	Global Settings	e	@rapidfiretools.com • 🔨
Sites 23 Q Search		All Site Types		+ Add Site
VS Site Test	~	Vulnerability Scanner 2021	~	
©	0	©	0	
VulScan Site 1	~			
	0			

- 3. All of your existing Inspector 2 sites will be migrated to VulScan sites in the **RapidFire Tools Portal**.
- 4. You an access these from [Your Site] > VulScan > Settings > Scan and

#### Notification Tasks.



## Next Steps for New VulScan Users

#### MORE INFO:

- **Documentation and downloads**: You can access VulScan documentation and downloads at <a href="https://www.rapidfiretools.com/vs-downloads">https://www.rapidfiretools.com/vs-downloads</a>
- Onboarding and customer success: Contact Customer Success at <u>customersuccess@rapidfiretools.com</u>, or sign up for training at <u>https://calendly.com/network-detective/vulscan-kickoff</u>
- Technical support: Contact Technical Support at <a href="mailto:support@rapidfiretools.com">support@rapidfiretools.com</a>

# Generate Internal Vulnerability Reports in Network Detective using VulScan

With your **Reporter** and/or **Network Detective Pro** subscription, you can use VulScan to generate internal vulnerability (**.ivul**) scan files for your assessments. This allows you to leverage VulScan to generate internal vulnerability reports in Network Detective. To do this:

1. First, you need to set up and manage VulScan scan tasks from the RapidFire Tools Portal. From Network Detective, when you right click **Manage** for a VulScan appliance from the site options, you will be prompted to access the portal.

#### **RapidFireTools**<sup>®</sup>

Active Project								
	Name	Type Man	nage Update	Remove	Running Tasks			
	KVS1-	Inspector 2.0 %	Manage 🎐 Update	🗙 Remove	No queued tasks			
	O KVS1-	Inspector 2.0 🍾	Manage 🌶 Update	🗙 Remove	No queued tasks			
	O KVS1-	Inspector 2.0 🍾	Manage 🗲 Update	🗙 Remove	No queued tasks			
Archived Projects Assessment-20210625								
	0% Complete 0 Complete	1) Required (1) Option	mal Created 25-Jun-202	1 11:03 AM Up	idated 25-Jun-2021	Manage KVS Settings		×
Progress Reports	Network Assessment	t (Domain) 0% Comp	plete 0 Complete 1	Required	1 Optional Or	To manage KVS settings, log	into the Your/TPortal and go to your sit	te.
Generated Reports	Run Network Detective Data Collector (NDDC) with the Network Scan	Computer Collector on puters that annot be need remot	ports			For Non-EU customers: For EU customers:	https://secure.youritportal.com https://secure.youritportal-eu.com	
Downloaded Reports	Double-click items to open.				l		Cancel	
	Run Network Dete Run the Network Data Col workstation on the network	ective Data Colle lector on the Domain Con c. The data collector sho	ector (NDDC) with ntroller (f possible), a comp suld be run with Administrat	the Netwo uter joined to the ive privileges.	rk Scan Domain if the Doma	ain Controller is not available, or from any		

2. When VulScan performs a successful internal vulnerability scan, you can click **Downland Scans**, select the .ivul file, and import it into your assessment.



- 3. You can then generate vulnerability scan reports using the Security module. Access this from the site reports console.
- 4. Select the relevant reports and click Create Reports.

Reports Create Reports	
All Reports V 33	% Available
Standard Reports	
Security Risk Report (.docx)	
Outhound Security Report (deex)	
Security Policy Assessment (docy)	
Share Permission Report (docy)	
Share Permission Report Excel (xlsx)	
Share Permission Report by User (docx)	
Share Permission Report by User Excel (xlsx)	
External Vulnerability Scan Detail Report (.docx)	
External Vulnerability Scan Detail by Issue Report	(.docx)
External Network Vulnerabilities Summary Report	(.docx)
External Vulnerability Scan Detail Excel (.xlsx)	
Internal Vulnerability Scan Detail Report (.docx)	
Internal Vulnerability Scan Detail by Issue Report	(.docx)
Internal Network Vulnerabilities Summary Report (	.docx)
Internal Vulnerability Scan Detail Excel (.xlsx)	
Login Failures by Computer Report (.docx)	
Login History by Computer Report (.docx)	
User Behavior Analysis Report (.docx)	
Anomalous Login Report (.docx)	
Security Assessment PowerPoint (.pptx)	

## VulScan and Reporter

While you manage VulScan from the RapidFire Tools Portal, it works the same way with Reporter as the previous (deprecated) Inspector 2 product. To use VulScan with

Reporter:

**Important:** After you migrate to VulScan, if a site with an equivalent name already exists in the RapidFire Tools portal and is being used for Cyber Hawk or Compliance Manager, a new site will be created with the suffix -VS (i.e., "My Site" would turn into "My Site-VS"). If you had a Reporter assigned to this site, you will need to manually move the Connector to the new site ("My Site-VS").

- 1. **Ensure your scan tasks have been created and scheduled** from your VulScan site in the RapidFire Tools Portal.
- 2. Ensure your Reporter internal vulnerability report tasks are set up and scheduled to occur after your scans will have finished. See the <u>Reporter User</u> Guide for Network Detective Pro.
- 3. Once your report task finishes, the reports will be available to download from the Reporter appliance as before.