

VECTR v7.0.2 Feature Breakdown

[Table of Contents](#)

Test Case Bulk Edit2

Test Case Bulk Edit

What is it?

From the Campaign screen, users can change attributes on multiple Test Cases at the same time.

How does it work?

From the Campaign screen, select multiple Test Cases using the checkboxes on the left, followed by clicking the “Edit” button:

SRB DEMO_PURPLE / Enterprise Purple – 2017 Q1 / External Port Scans

External Port Scans: Escalation Path

Reconnaissance

External - Moderate Port Scan with 10 ports, service enumeration, and NSE's

External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's

External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's

Timeline

01/03/2017 10:24:12
External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's : outcome changed to NotDetected





01/03/2017 09:02:11
External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's : status changed to Completed

01/03/2017 08:53:58
External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's : status changed to InProgress

01/03/2017 07:32:03
External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's : outcome changed to NotDetected

01/03/2017 06:17:35
External - Stealthy Port Scan with 3

Test Cases

	Phase	Technique	Test Case	Status	Outcome	Tags	Action
<input type="checkbox"/>	All	search ...	search ...	All	All	All	
<input checked="" type="checkbox"/>	Reconnaissance	Port scanning	External - Moderate Port Scan with 10 ports, service enumeration, and NSE's	Completed	Not Detected		   
<input checked="" type="checkbox"/>	Reconnaissance	Port scanning	External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's	Completed	Not Detected		
			External - Stealthy Port				

This will bring up the Bulk Edit screen. You can enable a field replacement by selecting the checkbox on the left followed by the appropriate action you want to perform. In the following, I'm going to add a tag called "Testing Tag" to both of the Test Cases:

Edit 2 Test Cases

☐ Replace with

Status: Completed

☐ Replace with

Attack Start

☐ Replace with

Attack Stop

☐ Replace with

Source IPs

☐ Replace with

Red Team Details

Technique

method

Phase

References

☐ Replace with

Attacker Tools

☐ Replace with

Nmap

☐ Replace with

Target Assets

☐ Replace with

Properties

☐ Replace with

Blue Team Details

Outcome

☐ TBD

☐ Blocked

☐ Detected

☒ NotDetected

Detecting Blue Tool(s):

Sub-Outcome

Was the event source logged?

☐ Yes

☒ TBD

☐ No

Outcome Notes

Tags

Testing Tag

Detection Time

Cancel

Save

After clicking “Save”, the edits will appear on the Campaign Screen:

The screenshot displays the 'Campaign Screen' for 'DEMO_PURPLE / Enterprise Purple - 2017 Q1 / Exter'. The top navigation bar includes 'SRA', 'Test Case Saved', and 'CLOSE' buttons. The main content area is divided into two sections: 'External Port Scans: Escalation Path' and 'Timeline'.

The 'External Port Scans: Escalation Path' section shows a diagram with a red arrow pointing to 'External Port Scans', which branches into three paths: 'Reconnaissance', 'External - Moderate Port Scan with 10 ports, service enumeration, and NSE's', 'External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's', and 'External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's'.

The 'Timeline' section shows a list of events with timestamps and descriptions:

- 01/03/2017 10:24:12: External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's : outcome changed to NotDetected
- 01/03/2017 09:02:11: External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's : status changed to Completed
- 01/03/2017 08:53:58: External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's : status changed to InProgress
- 01/03/2017 07:32:03: External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's : outcome changed to NotDetected
- 01/03/2017 06:17:35: (no description)

The 'Test Cases' section is a table with columns: Phase, Technique, Test Case, Status, Outcome, Tags, and Action. The table contains three rows of test cases, all with a status of 'Completed' and an outcome of 'Not Detected'. A red box highlights the 'Testing Tag' dropdown menu in the 'Tags' column.

Phase	Technique	Test Case	Status	Outcome	Tags	Action
Reconnaissance	Port scanning	External - Moderate Port Scan with 10 ports, service enumeration, and NSE's	Completed	Not Detected	Testing Tag	[Icons]
Reconnaissance	Port scanning	External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's	Completed	Not Detected	Testing Tag	[Icons]
Reconnaissance	Port scanning	External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's	Completed	Not Detected	[Icons]	[Icons]

How can this feature help me?

This allows for some of the more tedious processes of filling out Test Cases to be streamlined.