VECTR v7.0.2 Feature Breakdown

Table of Contents

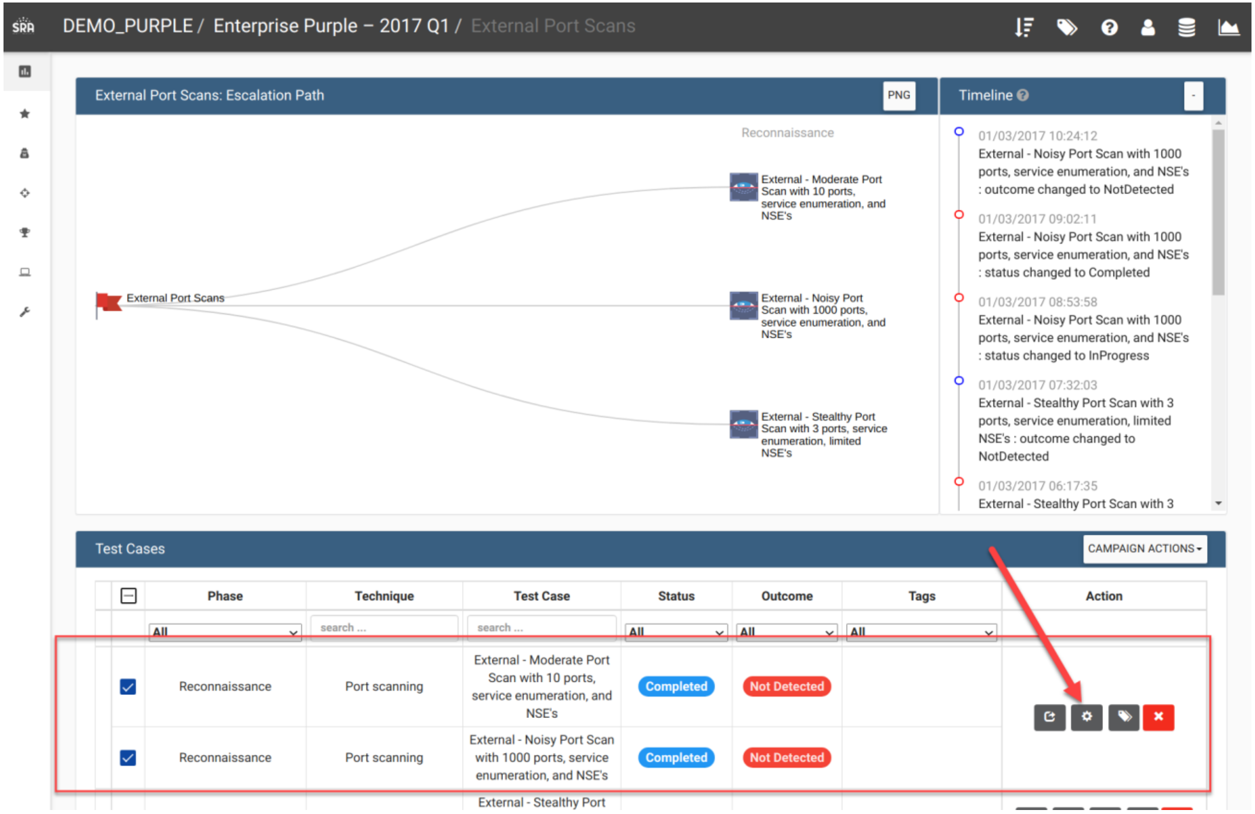
Test Case Bulk Edit

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:



DEMO_PURPLE / Enterprise Purple – 2017 Q1 / External Port Scans

External Port Scans: Escalation Path

PNG
Reconnaissance
External Port Scans
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

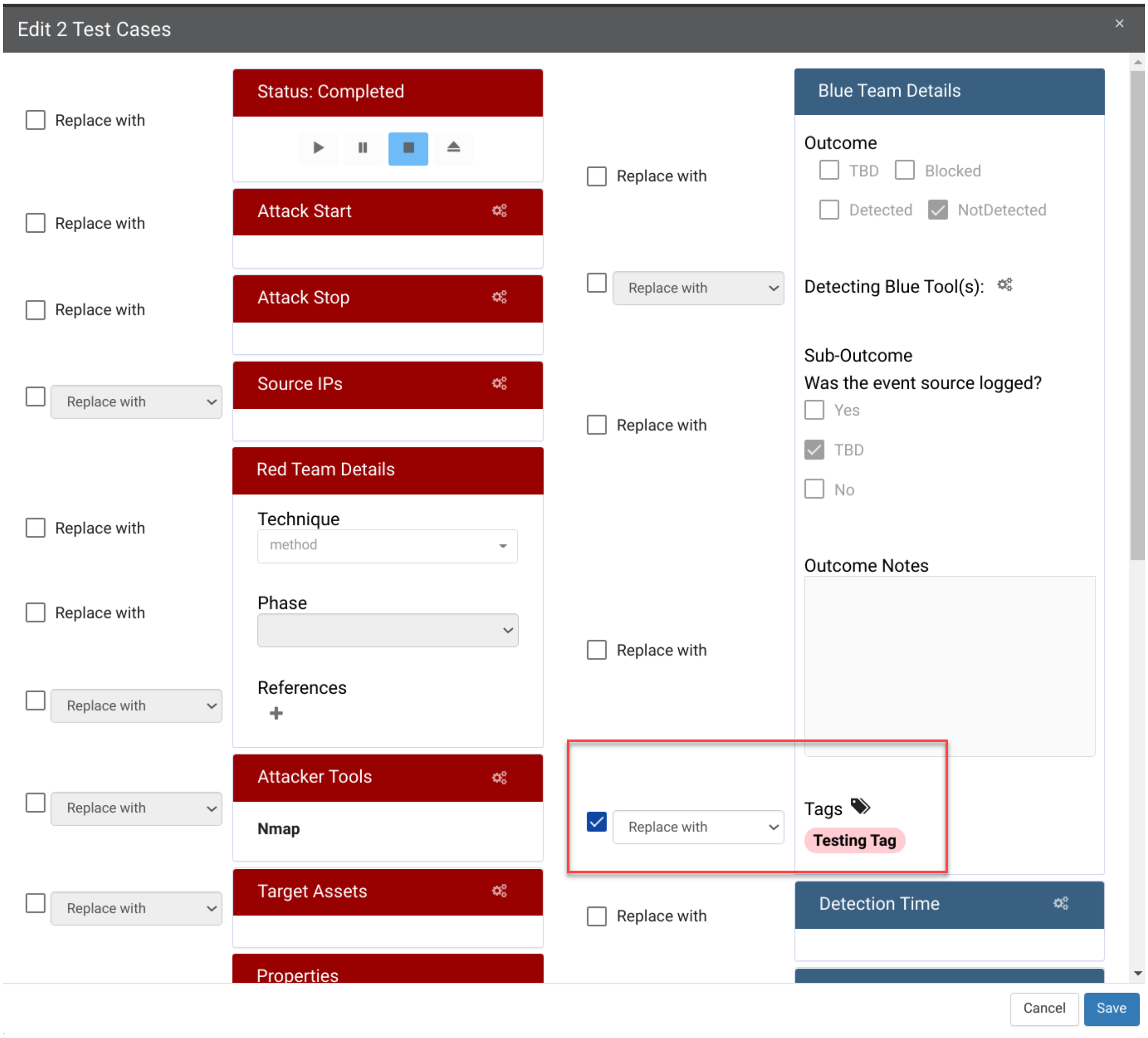
01/03/2017 07:32:03
External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's : outcome changed to NotDetected

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

Test Cases

⊟	Phase	Technique	Test Case	Status	Outcome	Tags	Action
	All	search ...	search ...	All	All	All	
☑	Reconnaissance	Port scanning	External - Moderate Port Scan with 10 ports, service enumeration, and NSE's	Completed	Not Detected		
☑	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

Red Team Details

□ Replace with — Technique: method

□ Replace with — Phase

□ Replace with — References

□ Replace with — Attacker Tools: Nmap

□ Replace with — Target Assets

Properties

Blue Team Details

□ Replace with — Outcome: □ TBD □ Blocked □ Detected ☑ NotDetected

□ Replace with — Detecting Blue Tool(s):

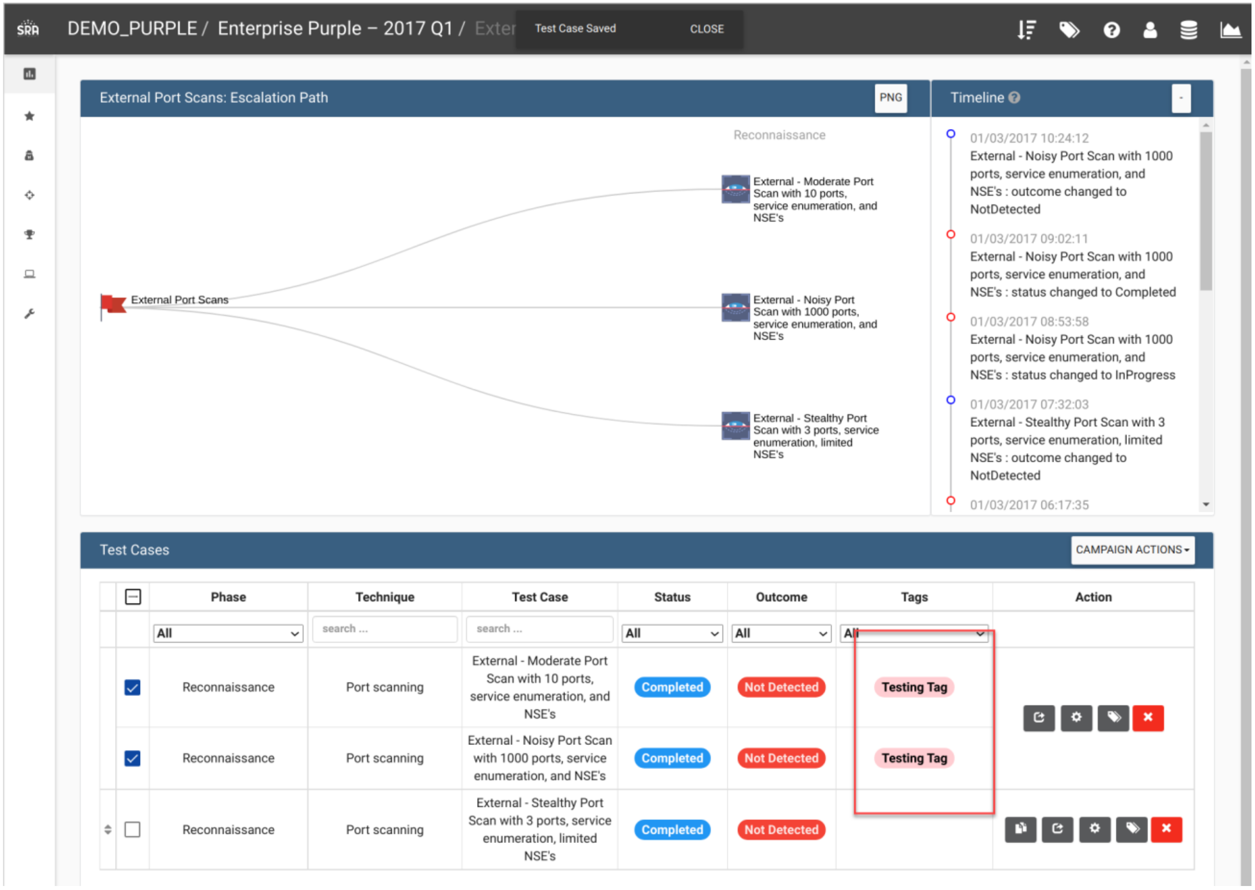
□ Replace with — Sub-Outcome
Was the event source logged?
□ Yes
☑ TBD
□ No

□ Replace with — Outcome Notes

☑ Replace with — Tags: Testing Tag

□ Replace with — Detection Time

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



DEMO_PURPLE / Enterprise Purple – 2017 Q1 / Exter
Test Case Saved
CLOSE
External Port Scans: Escalation Path
PNG
Reconnaissance
External Port Scans
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
Test Cases
CAMPAIGN ACTIONS

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

⊟	Phase	Technique	Test Case	Status	Outcome	Tags	Action
	All	search ...	search ...	All	All	All	
☑	Reconnaissance	Port scanning	External - Moderate Port Scan with 10 ports, service enumeration, and NSE's	Completed	Not Detected	Testing Tag	✖
☑	Reconnaissance	Port scanning	External - Noisy Port Scan with 1000 ports, service enumeration, and NSE's	Completed	Not Detected	Testing Tag	
□	Reconnaissance	Port scanning	External - Stealthy Port Scan with 3 ports, service enumeration, limited NSE's	Completed	Not Detected		✖

How can this feature help me?

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