GadgEon

Engineering Smartness

PENETRATION TESTING OF DATA CENTRE MONITORING APP

April,2020

Version 01

Penetration Testing of Data Center Monitoring Solution

Customer has developed a monitoring solution for their data center as they were experiencing difficulties due to the presence of many different hardware variants. End to end testing including non-functional testing like performance and vulnerability is complex and time consuming. The Customer was looking for automation of testing through automation.

Solution Description

- Gadgeon came up with a SOM-based solution with a homogenous HW/SW platform to cater to all variants of the customer's product. Monitoring and alarm handling system
- Gadgeon Test Automation Framework (GTF) was leveraged to automation of test cases and their convergence spanning across interfaces:- Web-UI , CLI , TL1, and SNMP
- Protocols Used : SNMP, TL1, TABS, TBOS, DCM ,HTTPS
- Tools Used : GTF based on Robot framework, Python, Selenium, TestRail, Jira, and Jenkins,
- Penetration Testing tools: OWASP and OpenVAS

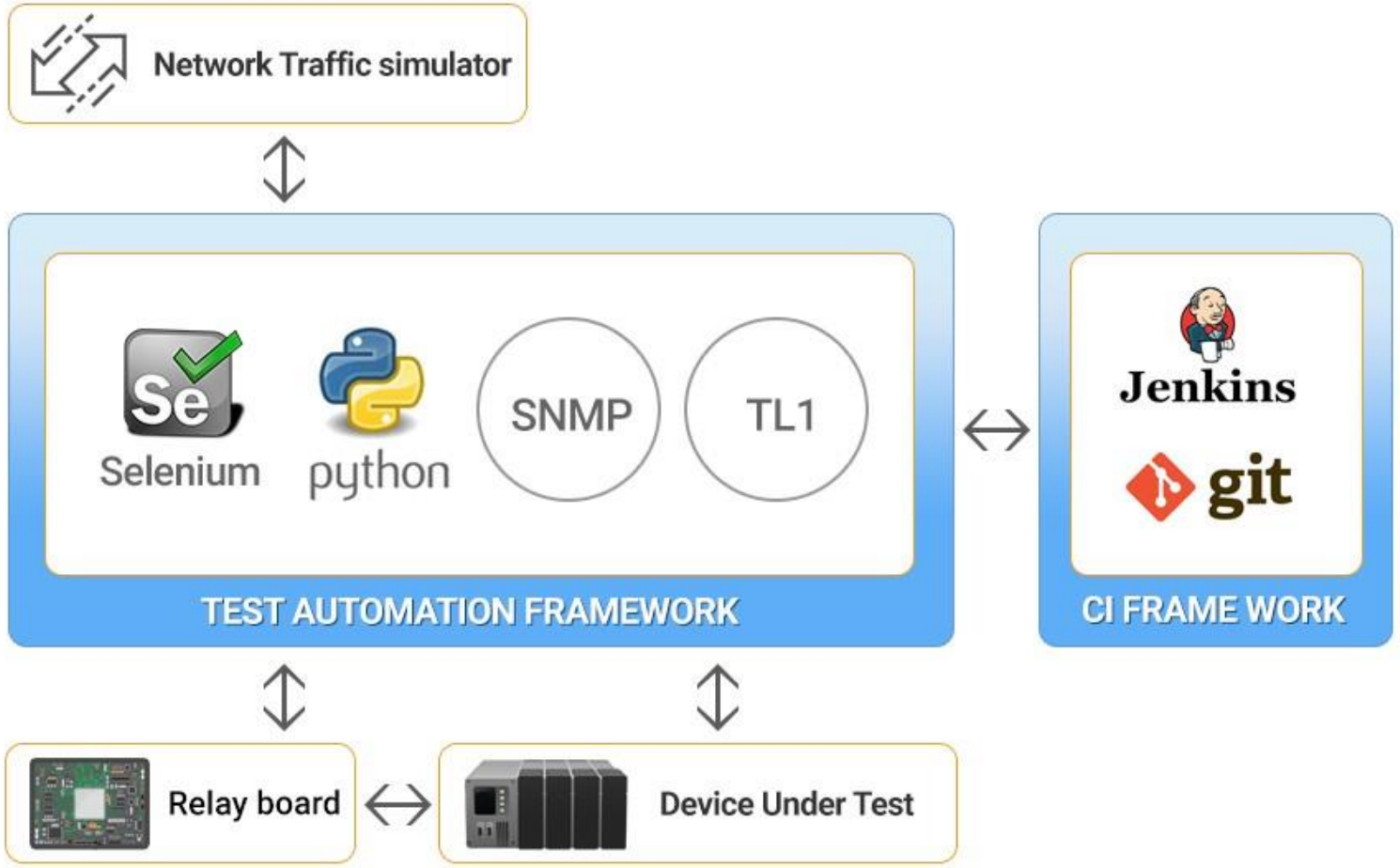
Outcome and Benefits Delivered

- Reduced the testing effort and schedule through automation of above 95% of regression, reliability, performance, and vulnerability test cases.
- Achieved 85 % of test coverage for functional test cases
- Achieved 100 % test coverage on regression test cases
- Achieved 90% test coverage for non-functional testing cases including its regression

The System Description

WHAT DID GADGEON DO?	PLATFORMS/TOOLS/TECHNOLOGIES USED
1) Defined Test Strategy for the complete system including different HW platforms with multiple communication protocols	Requirement Gathering & Analysis, defined functional test cases and uses case based on end to end test scenarios
2) Simulated high frequency polling conditions to stress the system	Python based custom stress scripts interfacing USB controlled relay
3) Designed Automation framework which can validate supporting protocols - SNMP, TL1, DCP/F, TBOS, TABS and DCM	NetSNMP Client for validating SNMP Commands and Operations Designed custom socket module for validating TL1, DCP/F, TBOS, TABS and DCM protocols Achieved 85 % of test coverage for functional test cases Achieved 100 % test coverage on regression test cases
4) Automated long duration stress test scripts for monitoring system health	Python based scripts monitoring CPU Utilization , Memory usage and communication interface stability
5) Automation framework supporting test evidence and detailed logs including screen shots for ease of debugging.	TestRail , Python, Appium , Selenium webdriver and Robot Framework
6) Security / Vulnerability testing	Owasp, OpenVAS, NMAP
7) Implemented Continuous Integration process as part of development and testing phases	Jenkins, Git, Robot Framework

The Solution / System Description



Tools / Technology Used

Device Automation
- Python , Selenium, SNMP, SSH, USB Controlled Relay , HTTPS

Continuous Integration
- Jenkins
- Git.

Test Management and Reports
- TestRail
- Robot Framework

Security/Vulnerability Testing
- OWASP
- OpenVAS

THANK YOU

For More Details, Let's Connect

Gadgeon Systems Inc.
881 Yosemite Way, Milpitas, CA 95035, USA

CONTACT - USA
Mani Ram - Vice President - Solutions and Technology
+1-678-900-0874 | mani.ram@gadgeon.com

Gadgeon Smart Systems Pvt Ltd.
Vl 405/E1, Fathima Tower, Maleppally Road, Thrikkakara PO,
Kochi, Kerala, PIN: 682021, India

CONTACT - INDIA
Hari Nair - CEO & Co-Founder
+91 989-501-5880 | hari.nair@gadgeon.com

Gadgeon Europe
Antwerpsesteenweg 124/54, 2630
Aartselaar, Belgium
+32 475 23 39 46 | europe@gadgeon.com

sales@gadgeon.com