2019 Employee Performance Goals

Gerard Sczepura

Software QA Analyst, Sr. Principal

Selenium

ASRC FEDERAL
Data Solutions

Education and Previous Experience

ASRC FEDERAL
Data Solutions

BS/MS Computer Science

Automated testing: 1985-2005

- Protocol Analyzer scripting – ± 5 yrs.
- Elverex EVALUATOR – 1 yr.
- QA Partner/SilkTest – 8 yrs.
- WinRunner – 1 yr.
- LoadRunner – 6 mos.
- QuickTest Pro – 1.5 yrs.

Dabbled in Selenium IDE and Selenium RC

Self-Study References

ASRC FEDERAL
Data Solutions

Primary:

- *Test Automation Using Selenium WebDriver 3.0 with C#*

  ISBN: 978-0-9922935-6-7, ©2018, $49.99 on Amazon
- https://www.seleniumhq.org/

Secondary:

Edureka! Selenium Tutorials:

- https://www.youtube.com/watch?v=5FUdrBq-WFo (Pt.#1)
- https://www.youtube.com/watch?v=ph3NJm4Z7m4 (Pt.#2)

Automation Assumptions and Concepts

ASRC FEDERAL
Data Solutions

Computer-Aided Software Testing (CAST)

- –IS NOT automated test case creation
- –IS automated test execution

All manual test activities still need to be performed:

- Test case design
- Test data creation
- Test verification

Automated script creation is a development activity!

Selenium Components

ASRC FEDERAL
Data Solutions

Selenium consists of the following components:

- WebDriver API
  - Communicates directly to the Browser
- Browser specific drivers or “enablers”
  - GeckoDriver, ChromeDriver, etc.
- Selenium Grid
- Selenium RC / Core
- Selenium IDE
  - Automation Recorder Extension for Firefox only

Katalon Recorder is a Selenium IDE-compatible replacement that supports both Firefox and Chrome.

Katalon Recorder

ASRC FEDERAL
Data Solutions

Katalon Recorder is a record and playback tool that is normally used for prototyping and object identification.

Chrome:

- https://chrome.google.com/webstore/search/katalon%20recorder%20selenium

Firefox:

- https://addons.mozilla.org/en-US/firefox/addon/katalon-automation-record/

Object Identification

ASRC FEDERAL
Data Solutions

Selenium WebDriver doesn't provide capabilities for identifying objects on a webpage.

- No Spy++

Katalon Recorder can be used to record actions on objects which exposes the objects' tag or locator information.

Locator information can also be obtained using the Inspector in the Browser's Web Developer or by viewing the page source.

- id, name, xpath, tag name, class name, link text, DOM, and CSS.

Visual Studio / C#

ASRC FEDERAL
Data Solutions

Microsoft Visual Studio Community 2017

- Universal Windows Platform development
- Office/SharePoint development
- Visual Studio Extension development
- .NET cross-platform development

Initially, the following NuGet Packages were installed:

- NUnit v3.12.0
- NUnit3TestAdapter v3.13.0
- Selenium.WebDriver v3.141.0
- Selenium.Support v3.141.0
- Selenium.WebDriver.GeckoDriver v0.24.0
- Selenium.WebDriver.ChromeDriver v75.0.3770.8

Verification Points

ASRC FEDERAL
Data Solutions

Verification Points or “Checkpoints” are steps coded in a test script that allow for the inspection of the application’s state.

Verification Points determine test case Pass/Fail criteria.

Verification Points are implemented using If-else and Assert statements.

- Console.Writeline() statements within if-else provide logging/reporting functionality.
- Assert statements are enclosed within try-catch blocks to prevent script termination upon detection of a failure.

Object Repository

ASRC FEDERAL
Data Solutions

Selenium WebDriver is an API not an application therefore the concept of an object repository doesn't exist.

- Examples: the WinRunner GUI Map and QuickTest Pro object repository

The automation tester can create their own object repository using a Shared UI Map similar to an application web.config file.

```
<appSettings>
    <add key="sUserName" value="username"/>
    .
    .
    .
</appSettings>
```

Script Generalization

ASRC FEDERAL
Data Solutions

Create functions for reusable code such as Login.

Use a configuration file (App.config) to deal with different environments or dynamic parameters.

- Multiple Shared UI Maps

Sample App.config:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings configSource="Configuration\SharedUIMap.config"></appSettings>
</configuration>
```

Data-Driven Tests

ASRC FEDERAL
Data Solutions

Read test data from an Excel spreadsheet.

- Similar to built-in QuickTest Pro data sheets.
- Each spreadsheet row, minus column header row, is a test case.

Again, WebDriver is an API not an application so the tester is responsible for “handling” the spreadsheet data.

The examples in the book used the NuGet package ExcelDataReader library to enable the test script to read Excel files.

Script Reliability Techniques

ASRC FEDERAL
Data Solutions

Synchronization

- Implicit/Explicit Wait

Pop-ups and modal dialogs

- IAlert interface

Parent/Child windows

- Interrogate open browser windows
- Obtain and use window handles to switch between windows

Dynamic Objects

- Parameterize the object's XPath value

Reporting

ASRC FEDERAL
Data Solutions

NUnit Console

- NuGet package: Nunit.Console
- Nunit3-console.exe

ReportUnit

- NuGet package: ReportUnit

Extent Reports

- NuGet package: Extent

Frameworks

ASRC FEDERAL
Data Solutions

Frameworks provide a standardized, consistent way to organize an automation environment.

Frameworks introduce additional levels of abstraction:

- Configuration files
- Functions
- External data repositories
  - Spreadsheet, database, etc.
- Keyword-driven
  - Hide complexity
  - Tool independent.

Assessment

ASRC FEDERAL
Data Solutions

An automation tester needs to possess the following skills to be successful in a C#/Visual Studio (or any other IDE) environment:

- Object-oriented programming: classes, methods
- IDE: navigation, structure, organization
  - VS NuGet, Eclipse packages
- Selenium Methods
- HTML/XML/XHTML
- Browser development tools
  - identify object properties, tags
- Debugging
- SQL
- Regular Expressions

Penetration Testing

Education and Previous Experience

ASRC FEDERAL
Data Solutions

No penetration testing experience

CompTIA Security+ certified

Completed the following Pluralsight related curricula:

- Network+
- Security+
- Ethical Hacker

Self-Study References

ASRC FEDERAL
Data Solutions

Primary:

- *Penetration Testing Essentials*

  ISBN: 978-1-119-23530-9, ©2017, $29.98 on Amazon

- *Learning Kali Linux: Security Testing, Penetration Testing, and Ethical Hacking*

  ISBN: 978-1-492-02869-7, ©2018, $35.78 on Amazon

Secondary:

- *Kali Linux Revealed: Mastering the Penetration Testing Distribution*

  ISBN: 978-0-9976156-0-9, ©2017, $26.99 on Amazon

Penetration Test Lab

ASRC FEDERAL
Data Solutions

Virtualization

- Sony VPC-EB290X Laptop, Windows 8.1 Pro, 8 GB RAM
- VMware Workstation 14 Player
  - Windows Server 2012 R2 core edition
  - Windows 2000 Pro
  - Windows Server 2000
  - Windows XP Pro

Kali Linux 64-bit (2019.3)

- LENOVO™ ideapad™ 310 Laptop, 12 GB RAM, Intel core i7, 238 GB Disk

Network

- Direct connect using a crossover cable (null modem)
- TP-Link switch

Steganography

Steganography is the process of hiding information within other objects such as images for example.

Used QuickStego for Windows to hide a text file in a JPEG image.

- 7.23 MB JPEG image
- 1 KB Text Document
- Bitmap image created with embedded text 8.6 MB

The next two slides contain screen shots of the original image and the image with the hidden text file. The two images appear identical with no discernable differences.

Steganography – Original Image

ASRC FEDERAL
Data Solutions

Steganography – Embedded Text Image

ASRC FEDERAL
Data Solutions

Network: Stress Testing

ASRC FEDERAL
Data Solutions

SYN flooding using *hping3*

In flood mode (*--flood*) SYN (*-S*) messages are sent to port 80 (*-p 80*) as fast as possible and as many as possible without waiting for responses.

The following output was generated for a run of only a few seconds to Windows Server 2012 R2 core edition.

```
root@kali:~# hping3 --flood -S -p 80 169.254.63.191
HPING 169.254.63.191 (eth0 169.254.63.191): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 169.254.63.191 hping statistic ---6349599 packets transmitted, 0 packets received, 100% packet lossround-
    trip min/avg/max = 0.0/0.0/0.0 ms
```

Port Scanning: Nmap

ASRC FEDERAL
Data Solutions

Scan entire network, scan all hosts from 169.254.63.0-255.

```
root@kali:~# nmap -sT -T 5 169.254.63.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2019-10-21 16:16 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
        specify valid servers with --dns-servers
Nmap scan report for 169.254.63.191
Host is up (0.0014s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
2179/tcp  open  vmrdp
49154/tcp open  unknown
MAC Address: 00:0C:29:E5:FB:3C (VMware)

Nmap done: 256 IP addresses (1 host up) scanned in 8.31 seconds
```

Vulnerability Scanning: OpenVAS

ASRC FEDERAL
Data Solutions

History

- Derived from Open Source Nessus fork
- Developed and maintained by Greenbone Networks

Install and Configure

- root@kali:~# apt install openvas
- root@kali:~# openvas-setup

Greenbone Security Assistant

- https://127.0.0.1:9392
- Admin User: admin
- Password: #########-####-####-####-8e3b97e56af4

OpenVAS Scan Results

Target ⇔ Windows Server 2012 R2

Abridged Scan Results

Security Issues for Host 192.168.0.37

Medium (CVSS: 5.0) 135/tcp

NVT: DCE/RPC and MSRPC Services Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736)

Summary

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

OpenVAS Scan Results

ASRC FEDERAL
Data Solutions

Abridged Scan Results cont'd

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Solution

Solution type: Mitigation

Filter incoming traffic to this ports.

Vulnerability Detection Method

Details: DCE/RPC and MSRPC Services Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736)

Version used: $Revision: 6319 $

Metasploit: Port Scanning

ASRC FEDERAL
Data Solutions

Target system: Server 2012 R2

```
msf5 > auxiliary/scanner/portscan/tcp > set rhosts 169.254.63.191/32
[-] Unknown command: auxiliary/scanner/portscan/tcp.
This is a module we can load. Do you want to use auxiliary/scanner/portscan/tcp? [y/N]   y
msf5 auxiliary(scanner/portscan/tcp) > set threads 10
threads => 10
msf5 auxiliary(scanner/portscan/tcp) > set CONCURRENCY 20
CONCURRENCY => 20
msf5 auxiliary(scanner/portscan/tcp) > set rhosts 169.254.63.191
rhosts => 169.254.63.191
msf5 auxiliary(scanner/portscan/tcp) > run
[+] 169.254.63.191:      - 169.254.63.191:135 - TCP OPEN
[+] 169.254.63.191:      - 169.254.63.191:2179 - TCP OPEN
[+] 169.254.63.191:      - 169.254.63.191:5985 - TCP OPEN
[*] 169.254.63.191:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Assessment

ASRC FEDERAL
Data Solutions

The *Learning Kali Linux* book was less theoretical and more practical than the *Penetration Testing Essentials* book.

Manual black box testers will find the transition to penetration testing challenging to say the least.

While many of the Kali Linux tools are GUI based, most are run from the command line.

Testers who are serious about learning penetration testing will eventually enroll in a course which provides them with exposure to a real world lab.