Sinhgad Institutes

SINHGAD TECHNICAL EDUCATION SOCIETY'S
SKN SINHGAD INSTITUTE OF TECHNOLOGY & TECHNOLOGY
Kusgaon(Bk), Lonavala 410401

DEPARTMENT OF COMPUTER ENGINEERING

LAB MANUAL
Academic year 2023-24

B.E. COMPUTER (SEM – I)

Laboratory Practice-IV (410247)

TEACHING SCHEME
PRACTICAL: 2 HRS/WEEK

EXAMINATION SCHEME
TERM WORK: 50 MARKS

Study material provided by: Vishwajeet Londhe

Join Community by clicking below links

Telegram Channel

https://t.me/SPPU_TE_BE_COMP

(for all engineering Resources)

SPPU Engineering & Technical UPDATES
WhatsApp channel

WhatsApp Channel

(for all Engg & tech updates)

https://whatsapp.com/channel/0029ValjFriICVfpcV9HFc3b

@SPPU_ENGINEERING_UPDATE

Insta Page

(for all Engg & tech updates)

https://www.instagram.com/sppu_engineering_update

Vision and Mission of Institute

VISION

उत्तमपुरुषान् उत्तमाभियंतृन् निर्मातुं कटीबध्दा: वयम्।

We are committed to produce not only good engineers but good human beings, also.

MISSION

Holistic development of students and teachers is that we believe in and work for, We strive to achieve this by imbibing a unique value system, transparent work culture, excellent academic and physical environment conducive to learning, creativity and technology transfer. Our mandate is to generate, preserve and share knowledge for developing a vibrant society.

Vision and Mission of Department

VISION

We strive to produce globally competent computer professionals enriched with innovative skills and good moral values with societal concerns.

MISSION

M1: To provide broad-based education and contemporary knowledge by Adopting modern teaching-learning methods.

M2: To inculcate a spirit of innovation in students through industrial interactions.

M3: To develop individual's potential to its fullest extent so that they can emerge as gifted leaders in their fields.

Short Term Goals

- To establish post graduate program in different domain.
- To encourage faculty by creating opportunity of higher education.
- To initiate relevant value addition programs and certifications for improving employability.
- Build strong alliances that bring know-how of business community to complete training of students through projects.

Long Term Goals

- To establish a center of innovation in Agriculture, Tele health and ICT sector in collaboration with industry.
- To create center of excellence in network, security and computer vision.
- To establish a world class R&D institute for patent based research creating opportunity for faculty to be resource.

Program Educational Objectives (PEO's)

1. To prepare globally competent graduates having strong fundamentals and domain knowledge to provide effective solutions for engineering problems.
2. To prepare the graduates to work as a committed professional with strong professional ethics and values, sense of responsibilities, understanding of legal, safety, health, societal, cultural and environmental issues.
3. To prepare committed and motivated graduates with research attitude, lifelong learning, investigative approach, and multidisciplinary thinking.
4. To prepare the graduates with strong managerial and communication skills to work effectively as individual as well as in teams.

Program Outcomes: POs

Students are expected to know and be able –

PO1- *Engineering Knowledge*: - To apply knowledge of mathematics, science, engineering fundamentals, problem solving skills, algorithmic analysis and mathematical modelling to the solution of complex engineering problems.

PO2- *Problem Analysis*: - Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusion using first principals of mathematics, natural sciences and engineering sciences.

PO3- *Design / Development of solutions*: - Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate considerations for the public health and safety, and the cultural, social and environmental considerations.

PO4- *Conduct Investigations of Complex Problems*: - Use research based knowledge and research methods including design of experiments, analysis and interpretation of data, and modeling to complex engineering activities with an understanding of the limitations.

PO5- *Modern Tool Usage*: - Create, select and apply appropriate techniques, resources and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6- *the Engineer and Society*: - Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7- *Environment and Sustainability*:- Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8- *Ethics*:- Apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practice.

PO9- *Individual and Team work* :-Function effectively as an individual and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10- *Communication Skill*:- Communicate effectively on complex engineering activities with the engineering community and with society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive dear instructions.

PO11- *Project management Finance*: - Demonstrate knowledge and understanding of engineering and management principles and apply these to one's own work as a member and leader in a team to manage projects and in multidisciplinary environment.

PO12- *Life-long Learning*: - Recognize the need for, and have the preparations and ability to engage in independent and lifelong learning in the broadest context of technological change.

Program Specific Outcomes: PSOs

A graduate of the Computer Engineering Program will demonstrate-

PSO1-*Professional Skills*-The ability to understand, analyze and develop computer programs in the areas related to algorithms, system software, multimedia, web design, big data analytics, and networking for efficient design of computer-based systems of varying.

PSO2-*Problem-Solving Skills*- The ability to apply standard practices and strategies in software project development using open-ended programming environments to deliver a quality product for business success.

PSO3-*Successful Career and Entrepreneurship*- The ability to employ modern computer languages, environments, and platforms in creating innovative career paths to be an entrepreneur, and a zest for higher studies.

Course Objectives:

Learn android application development related to pervasive computing

- Understand various multimedia file formats
- Understand various vulnerabilities and use of various tools for assessment ofvulnerabilities
- Understand information retrieval process using standard tools available
- Learn GPU programming and implementation of same using open sourcelibraries
- Learn installation and use of open source software testing tools

Course Outcomes:

After completion of the course, students will be able to

CO1: Apply android application development for solving real life problems
CO2: Design and develop system using various multimedia components.
CO3: Identify various vulnerabilities and demonstrate using various tools.
CO4: Apply information retrieval tools for natural language processing
CO5: Develop an application using open source GPU programming languages
CO6: Apply software testing tools to perform automated testing

Sinhgad Institutes

SKN SINHGAD INSTITUTE OF

TECHNOLOGY & SCIENCE

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that, Mr. /Miss _____of class BE

Roll No._____Exam Seat No._____

Has completed all the practical work in the subject *Laboratory Practices-IV*, satisfactorily, as prescribed by Savitribai Phule Pune University, Pune (SPPU) in the Academic Year 2023-24.

Subject In-charge	Head of Department
Dr. S. M. Patil	Dr. S.M.Patil

Guidelines for Laboratory /Term Work Assessment

Continuous assessment of laboratory work is based on overall performance and Laboratory assignments performance of student. Each Laboratory assignment assessment will assign grade/marks based on parameters with appropriate weightage. Suggested parameters for overall assessment as well as each Laboratory assignment assessment include- timely completion, performance, innovation, efficient codes, punctuality and neatness

Guidelines for Laboratory Conduction

The instructor is expected to frame the assignments by understanding the prerequisites, technological aspects, utility and recent trends related to the topic. The assignment framing policy needto address the average students and inclusive of an element to attract and promote the intelligent students. The instructor may set multiple sets of assignments and distribute among batches of students. It is appreciated if the assignments are based on real world problems/applications. Use of open source software is encouraged.In addition to these, instructor may assign one real life application in the form of a mini-project based on the concepts learned. Instructor may also set one assignment or mini-project thatis suitable to respective branch beyond the scope of syllabus.

Guidelines for Oral Examination

. During oral assessment, the expert evaluator should give the maximum weightage to the satisfactory implementation of the problem statement. The supplementary and relevant questions may beasked at the time of evaluation to test the student’s for advanced learning, understanding of the fundamentals, effective and efficient implementation. So encouraging efforts, transparent evaluation andfair approach of the evaluator will not create any uncertainty or doubt in the minds of the students. So adhering to these principles will consummate our team efforts to the promising start of the student's academics.

SINHGAD INSTITUTE OF TECHNOLOGY, LONAWALA.

Department of Computer Engineering

Laboratory Practice-IV BE Computer Engineering

Group A (Cyber security & Digital forensics)	
1	Write a program for Tracking Emails and Investigating Email Crimes. i.e. Write a program to analyze e–mail header.
2	Implement a program to generate and verify CAPTCHA image.
3	Write a computer forensic application program for Recovering permanent Deleted Files and Deleted Partitions.
4	Write a program for Log Capturing and Event Correlation.
5	Study of Honeypot.
Group B (Cyber security & Digital forensics-Mini Project)	
6	**Mini Project** : Design and develop a tool for digital forensic of images
Group C (Software Testing &Quality Assurance)	
7	Write TEST Scenario for Gmail Login Page.
8	Write Test cases in excel sheet for Social Media application or website.
9	Create Defect Report for Any application or web application.
10	Installation of Selenium grid and selenium Web driver java eclipse (automation tools).
11	Prepare Software requirement specification for any project or problem statement.
Group D (Software Testing &Quality Assurance-Mini Project)	
12	**Mini Project :**Software Testing and Quality Assurance Mini Project Dynamic website of covid- 19 information using HTML, CSS, JAVASCRIPT And PHP, MySQL database used to store user account, comment, and registration form details. Regular Expression testcases for testing Purpose.

Assignment No: 1

Title: Tracking and Investigating Email Crimes.

Problem Statement: Write a program for Tracking Emails and Investigating Email Crimes. i.e. Write a programto analyze e–mail header.
Objectives: To track and investigate email crimes.

Theory: Emails play a very important role in business communications and have emerged as one ofthe most important applications on internet. They are a convenient mode for sending messages as well as documents, not only from computers but also from other electronic gadgets such as mobile phonesand tablets.
The negative side of emails is that criminals may leak important information about their company. Hence, the role of emails in digital forensics has been increased in recent years. In digital forensics, emails are considered as crucial evidences and Email Header Analysis has become important to collect evidence during forensic process.
An investigator has the following goals while performing email forensics −

To identify the main
criminal To collect
necessary evidencesTo
presenting the findings
To build the case
Email forensics is the study of source and content of email as evidence to identify the actual sender and recipient of a message along with some other information such as date/time of transmission and intention of sender. It involves investigating metadata, port scanning as well as keyword searching.
Some of the common techniques which can be used for email forensic investigation are

Header Analysis
Server investigation
Network Device Investigation
Sender Mailer Fingerprints
Software Embedded Identifiers

To understand email header fields in Gmail, we take a message of a sender as an example.

```
Delivered-To: paul.friedman@gmail.com
Received: by 10.12.174.216 with SMTP id n34csp2326299qvd;
        Wed, 1 Feb 2017 00:39:09 -0800 (PST)
X-Received: by 10.28.27.14 with SMTP id b14mr1702258wmb.82.1485938349292;
        Wed, 01 Feb 2017 00:39:09 -0800 (PST)
Return-Path: <reply@activetrail.com>
Received: from i2.a01.ms18.atmailsvr.net (i2.a01.ms18.atmailsvr.net.
[91.199.29.18])
        by mx.google.com with ESMTPS id
5si23398790wrr.176.2017.02.01.00.39.08
        for <paul.friedman@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 01 Feb 2017 00:39:09 -0800 (PST)
Received-SPF: pass (google.com: domain of reply@activetrail.com designates
91.199.29.18 as permitted sender) client-ip=91.199.29.18;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@activetrail.com;
       spf=pass (google.com: domain of reply@activetrail.com designates
91.199.29.18 as permitted sender) smtp.mailfrom=reply@activetrail.com;
       dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=gingersoftware.com
X-IADB-IP: 91.199.29.18
X-IADB-IP-REVERSE: 18.29.199.91
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; q=dns/txt;
d=activetrail.com; s=at; h=X-BBounce:X-IADB-URL:Sender:Submitter:X-
Feedback-ID:From:To:Date:Subject:MIME-Version:Content-type:Content-
Transfer-Encoding; bh=GytDyTyaDleCfGk0d7bL4F2bXbTuWsb/xtpIVyVaCRw=;
b=sgh6nUFjt5FC7rBC2BwXFulNuG+k14R7bBsstb4erjtZfTn4z/NPHNhVb4Ax1yXoOgX+
Il6n5SCcXTCkwQdmaxpxt/BzPjWVziBdzU1WichHhPabVFeKctyp6pCjv4+d2FVIiEuxqi
v5dBTcJjXBVpOwU0mqgRceh3pqcvd5Rj4=
```

By analyzing the key parameters in an email header, you can get an idea of how the message traveled from the source to the destination. For instance, you can use the originating IP to find the original sender. For this, you need to examine the first Received parameter in the email header. The first IP address here is the originating IP which is also sometimes presented in the fields X- Originating-IP or Original-IP. Borrowing the same header example:

```
Received: by 10.12.174.216 with SMTP id n34csp2326299qvd; Wed, 1 Feb 2017 00:39:09 -0800
(PST)
```

The highlighted portion is the original sender of the message. You can use a free reputation service like SenderBase by Cisco to get the reputation rating of the IP. This can help ascertain whether the email is spam or a phishing attack. Although, bear in mind that if the IP address is private, then itmay not fetch any result. Message-ID is another important field that can be checked during email header analysis for spoofing. You can see it below in the highlighted region.

```
Reply-To: Newsletter@gingersoftware.com
From: Ginger (noreply@gingersoftware.com)
To: "paul.friedman@gmail.com" (paul.friedman@gmail.com)
Message-ID: (c000e5f41f8f4137a30cab4g6eddcd1e@gingersoftware.com)
```

- Date: Wed, 01 Feb 2017 10:39:06 +0200
- Subject: Thank you for registering with Ginger!
- MIME-Version: 1.0

Since Message-ID is added by the mail server that processes the email, it can't be altered. Also,message systems often use a date/time stamp, along with the sender's domain name. So, if the domain name in the message ID doesn't match the domain name mentioned in the From: field, then it can suggest a possibility of spoofing. In the example above, the From: field shows the domain name gingersoftware.com, which is same as the Message ID. So, it's safe to assume that no spoofing took place here.

Before you can analyze an email header, you first need to obtain it. Here‘s how to do that in Gmail:

Open Gmail.

Find the message you want to analyze.

Click the three vertical dots in the upper-right of the message.

Click ―Show Original.‖

Here, you‘ll see a brief breakdown of the information found in the header. If you scroll down, youcan also see the full text of the email header, which will end just before the body content of the message.

From there, you can copy the email header into an email header analysis tool to learnmore details.

How to Analyze Email Headers in Outlook

Here‘s how to obtain your email header in Outlook:

1. Open Microsoft Outlook.
2. Click on the message you want to analyze.
3. Click on the dropdown arrow in the upper-right of the message.
4. Click ―View message details.‖

Here, you‘ll see the full text of the email header.

From there, you can copy the email header into an email header analysis tool to learn more details.

Email Header Analyzer Tools

Once you have a copy of the email header, you can analyze it using one of the following email header analysis tools.

Almost all of these tools are free, and function in the same way, so I won‘t go into detail describing the minor differences. With all of them, you‘ll copy and paste your email header, click a button, and review theinformationafter it is parsed.

1. **G Suite Toolbox Messageheader.**

If you're already using Gmail, you might as well try G Suite's Messageheader tool.

2. **Mx Toolbox.**

Mx Toolbox has a great standalone email header analyzer, as well as detailed information on email headers for the uninitiated.

3. **What Is My IP?**

We've already credited them for their helpful email examples, but What Is My IP also has a convenient email header analysis tool.

4. **Mailheader.org.**

There's also Mailheader.org, where you can review mail header samples in addition to the header you've selected.

5. **Gaijin.**

In case you needed more options, you could also try Gaijin.

If the above email header analyzer tools return an error message or if there's a bit of information you were unable to find in their analysis, consider manually reviewing the email headers yourself.

Conclusion: Thus we can track and Investigate Email Crimes.

Assignment No: 2

Problem Statement: Implement a program to generate and verify CAPTCHA image.

Objectives: To implement a program to generate and verify CAPTCHA image.

Theory:

To generate captchas using Python following are the steps:

Install The Captcha Module

So just like any other program, the very first step is to install the CAPTCHA library. In order to do that openyour command prompt and run the following command:

pip install captcha

Steps to Create Captcha Generator in Python

We would try to generate both images as well as audio captchas in this tutorial. Hence, when you are done installing the library, you need to import the ImageCaptcha and AudioCaptcha functions from captcha.image andcaptcha.audio sub-libraries respectively

```
1  from captcha .image import
   Image Captcha

2  from captcha. audio import
   Audio Captcha
```

Generating Image Captcha in Python

Let's start by creating an Image captcha. We will be taking input about the text that needs to display on the screen from the user and then generate the image captcha for the data.

To create the captcha, we need to create an Imagecaptcha object and then generate the captcha for the data using the generate function. Look at the code below.

```
1    img = ImageCaptcha(width  = 280, height = 90)text =
2    input("Enter the Text for Captcha: ")
3    Cap_data = img.generate(text)
```

The image is generated but to save the image we need to use the write function using the code below. img.write(text,

'Sample_Cap_1.png')

C++ code:

We are using rand() to generate CAPTCHA randomly.

1. Create a function generateCaptcha that generate a CAPTCHA of length n Create an empty string captcha to store the generated captcha.

use rand() function to add characters to the captcha.

2. Now get the user input.
3. Use compare() function to compare the generated captcha with user input.#include <bits/stdc++.h> using

```
namespace std;
// function to check user input to generated CAPTCHA bool
check_Captcha(string &captcha, string &user_input){
        return  captcha.compare(user_input)  ==  0;
}
```

```
// function to generate CAPTCHA of length nstring generateCaptcha(int n){
        time_t t; srand((unsigned)time(&t));
    char  *required_chars  = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";  string
        captcha =  "";
        while(n--)
           captcha.push_back(required_chars[rand()%62]);  return
        captcha;
}
     int main(){
        int n;
        cout<<"Enter the required length of CAPTCHA: ";cin>>n; string
                captcha     =     generateCaptcha(n);
        cout<<"CAPTCHA: "<<captcha<<endl; string user_input;
        cout<<"Enter     the     CAPTCHA:     ";
        cin>>user_input;
        if     (check_Captcha(captcha,     user_input))
           cout<<"Valid CAPTCHA"<<endl;
        else
           cout<<"Invalid  CAPTCHA"<<endl;
        return  0;
}
```

Output:

```
Enter the required length of CAPTCHA: 6CAPTCHA:
OsBVxh
Enter the CAPTCHA: OsBVxh
Valid CAPTCHA

Enter the required length of CAPTCHA: 8CAPTCHA:
R5y3cVuW
Enter the CAPTCHA: R5y3cVuW
Valid CAPTCHA

Enter the required length of CAPTCHA: 5CAPTCHA:
Y3EgK
Enter the CAPTCHA: y3egk Invalid
CAPTCHA
```

Conclusion: Thus we have implemented a program to generate and verify CAPTCHA image.

Assignment No: 3

Problem Statement: Write a computer forensic application program for recovering permanent deleted files and deleted partitions.

Objectives: To write a computer forensic application program for recovering permanent deleted files and deleted partitions.

Theory:

Destroyed Evidence

In a criminal or cyber-criminal case, the attempts to destroy the evidence are very common. Such attempts can be more or less successful depending upon the following conditions:

- Action is taken to destroy the evidence.
- Time Available to destroy the evidence.
- Type of storage device like magnetic hard drive, flash memory card, or SSD drive.

Deleted Files

Deleting files is one of the easiest, convenient, and foremost way to destroy the evidence. Whether it is using the ―Delete‖ button or ―Shift+Delete‖ button. The principle of file recovery of deleted files is based on the fact that Windows does not wipe the contents of the file when it's being deleted.

Instead, a file system record storing the exact location of the deleted file on the disk is being marked as ―deleted‖ and the disk space previously occupied by the deleted file is then labeled as available – but not overwritten with zeroes or other data.

- The deleted file can be retrieved by analyzing the contents of the recycle bin as they are temporarily stored there before being erased.
- If the deleted files have no trace in the recycle bin like in case of the ―Shift+Delete‖ command, then, in that case, you can use commercial recovery tools to recover the deleted evidence. One such example commercial tool is Disk Internals Partition Recovery.
- Looking for characteristic signatures of known file types by analyzing the file system and/or scanning the entire hard drive, one can successfully recover :
    - Files that were deleted by the user.
    - Temporary copies of Office documents (including old versions and revisions of such documents).
    - Temporary files saved by many applications.
    - Renamed files.

Formatted Hard Drives:

Recovery of the data from the formatted hard drive depends upon a lot of parameters. Information from the formatted hard drive may be recoverable either using data carving technology or by using commercial data recovery tools.

There are two possible ways to format a hard drive: **Full Format and Quick Format**.

Full Format – As the name suggests, this initializes the disk by creating the new file system on the partition being formatted and also checks the disk for the bad sectors. Prior to Windows Vista, a full format operationdid not zero the disk being formatted. Instead, Windows would simply scan the disk surface sector after sector. Unreliable sectors would be marked as ―bad‖. But in case of Vista and Windows 7, a full format operation willactually:

- Wipe the disk clean.
- Writing zeroes onto the disk.
- Reading the sectors back to ensure reliability.

Quick Format – This is never destructive except for the case of SSD. Disk format simply initializes the disk by creating the new file system on the partition being formatted. Information from disks cleared using a quick format method can be recovered by using one of the data recovery tools thatsupport data carving.

SSD Drives

SSD means Solid-State Drives represent a new storage technology.

- They operate much faster than traditional drives.
- They employ a completely different way of storing information internally, which makes it much easier to destroy information and much more difficult to recover it.

The culprit in SSD is **TRIM Command**. According to a survey, TRIM enables SSD completely wiped all the deleted information in less than 3 minutes. This means that the TRIM command effectiv ely

zeros all the information as soon as it is marked as deleted by the operating system. Moreover, TRIM command effects can‘t be prevented even by using Write-Blocking devices.

Traditional Methods are not useful when we try to recover deleted data from the SSD or even any information from the SSD formatted with either Full format or Quick format. This means the traditional methods can be used for data recovery in SSD only when the TRIM command is not issued or atleast one of the components does not support TRIM. The components include:

- **Version of Operating System:** Windows Vista and Windows 7 support TRIM Command, on the other hand, Windows XP and earlier versions typically don‘t support TRIM Command.
- **Communication Interface:** SATA and eSATA support TRIM, while external enclosures connected via USB, LAN or FireWire don‘t.
- **File System:** Windows supports TRIM on NTFS volumes but not on FAT-formatted disks. Linux, on the other hand, supports TRIM on all types of volumes including those formatted with FAT.

Conclusion: Thus we have studied to write a computer forensic application program for recovering permanent deleted files and deleted partitions.

Assignment No: 04

Problem Statement: Write a program for log capturing and event correlation.

Objectives: To write a program for log capturing and event correlation.

Theory:

What is log capturing?
The logs generated by any system are stored in files which are called as log files.
We can retrieve this information using various system commands which is called _Log Capturing'.
Linux systems have a very flexible and powerful logging system, which enables you to record almostanything you can imagine and then manipulate the logs to retrieve the information you require. Linuxuses a set of configuration files, directories, programs, commands and daemons to create, store andrecycle these log messages.

Need of log capturing:
Linux system administrators often need to look at log files for troubleshooting purposes.
Knowing where the system keeps its log files and how to make use of related commands can therefore help save valuable time during troubleshooting.
It helps to monitor the system performance.
From security point of view the events logged in the log file are mainly:

1. Authentication attempts – both successful and failed.
2. All bad requests – which includes attempts for SQL injections and various hacking efforts. Helps to monitor and check resource allocation and usage

Log capturing in Linux:

At the heart of the logging mechanism is the rsyslog daemon. This service is responsible for listening to log messages from different parts of a Linux system and routing the message to an appropriate log file in the /var/log directory.

The rsyslog daemon gets its configuration information from the rsyslog.conf file. The rsyslog.conf file is found in the /etc directory. This instruction comes from a series of two-part lines within the file. The two part instruction is made up of a selector and an action. The two parts are separated by white space.

1) auth or authpriv: Messages coming from authorization and security related events.

2) kern: Any message coming from the Linux kernel.

3) mail: Messages generated by the mail subsystem.

4) cron: Cron daemon related messages.

5) daemon: Messages coming from daemons.

6) news: Messages coming from network news subsystem.

7) lpr: Printing related log messages.

8) user: Log messages coming from user programs.

9) local0 to local7: Reserved for local useLinux

Commands Used:

top - top provides an ongoing look at processor activity in real time. It displays a listing of the most CPU-intensive tasks on the system, and can provide an interactive interface for manipulatingprocesses.

who – shows who is logged in.

last – shows listing of last logged in users, last searches back through the file /var/log/wtmp anddisplays a list of all users logged in since that file was created.

lastlog - reports the most recent login of all users or of a given user, lastlog formats and prints the contents of the last login log /var/log/lastlog file.

last reboot - to find out when was the system last rebooted.

strace - In the simplest case strace runs the specified command until it exits. It intercepts and recordsthe system calls which are called by a process and the signals which are received by a process. Thename of each system call, its arguments and its return value are printed on standard error or to the file specified with the -o option.

cat - concatenate files and print on the standard output.

system() - The C library function int system(const char *command) passes the command name or program name specified by command to the host environment to be executed by the command processor and returns after the command has been completed

Conclusion: Thus we have studied log capturing and event correlation.

Assignment No: 5

Title: Honeypot

Problem Statement : Study of Honeypot..

Objectives: To Study of Honeypot**. Theory:**

Honeypots

A honeypot is an "an information system resource whose value lies in unauthorized or illicit use of that resources"

"A server that is configured to detect an intruder by mirroring a real production system. It appears as an ordinary server doing work, but all the data and transactions are phony. Located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques as well as determine vulnerabilities in the real system"

Honeypot History

The first publically available honeypot was Fred Cohen's Deception ToolKit in 1998 which was "intended to make it appear to attackers as if the system running DTK [had] a large number of widely known vulnerabilities" More honeypots became both publically and commercially available throughout the late nineties. As worms began to proliferate beginning in 2000, honeypots proved imperative in capturing and analyzing worms. In 2004, virtual honeypots were introduced which allow multiple honeypots to run on a single server.

Types of Honeypots

There are two broad categories of honeypots available today, high-interaction and low-interaction. These categories are defined based on the services, or interaction level, provided by the honeypot to potential hackers .**High-interaction honeypots** let the hacker interact with the system as they would any regular operating system, with the goal of capturing the maximum amount of information on the attacker's techniques. Any command or application an end-user would expect to be installed is available and generally, there is little to no restriction placed on what the hacker can do once he/she comprises the system. On the contrary, **low-interaction honeypots** present the hacker emulated services with a limited subset of the functionality they would expect from a server, with the intent of detecting sources of unauthorized activity.

General Honeypot Advantages and Disadvantages

Honeypots provide several advantages over other security solutions, including network intrusion detection systems:

- Fewer false positives since no legitimate traffic uses honeypot
- Collect smaller, higher-value, datasets since they only log illegitimate activity
- Work in encrypted environments
- Do not require known attack signatures, unlike IDS

Honeypots are not perfect, though:

- Can be used by attacker to attack other systems
- Only monitor interactions made directly with the honeypot - the honeypot cannot detect attacks against other systems
- Can potentially be detected by the attacker

Tradition security solutions, such as intrusion detection systems, may not be enough in light of more complicated attacks. Honeypots provide a mechanism for detecting novel attack vectors, even in encrypted environments. Advances such as virtualization have made honeypots even more effective. Honeypots have drawbacks, though, so it is important to understand how honeypots operate in order to maximize their effectiveness.

Honeynets and Honeyfarms

Honeynets and honeyfarms are the names given to groups of honeypots. Honeyfarms tend to be more centralized. Grouping honeypots provide many synergies that help to mitigate many of the deficiencies of traditional honeypots. For instance, honeypots often restrict outbound traffic in order to avoid attacking non-honeypot nodes. However, this restriction allows honeypots to be identified by an attacker. He et al. use honeyfarms as redirection points for outbound traffic from each individual honeypot. These redirection nodes also behave like real victims Figure 1 shows the redirection of outbound traffic from a honeypot to another node in the honeyfarm.

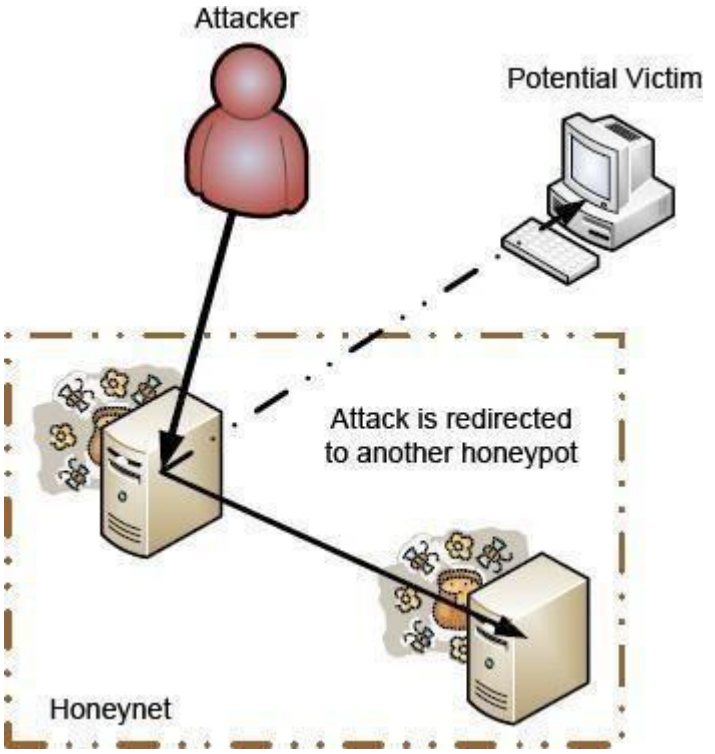


Figure 1. Redirecting an outbound attack in a honeynet

Shadow honeypots are combination of honeypots and anomaly detection systems (ADS), which are another alternative to rule-based intrusion detection systems.

Shadow honeypots first segment anomalous traffic from regular traffic. The anomalous traffic is sent to a shadow honeypot which is an instance of a legitimate service as shown in Figure 2. If an attack is detected by the shadow honeypot, any changes in state in the honeypot are discarded. If not, the transaction and changes are correctly handled. While shadow honeypots require more overhead, they are advantageous in that they can detect attacks contingent upon the state of the service.

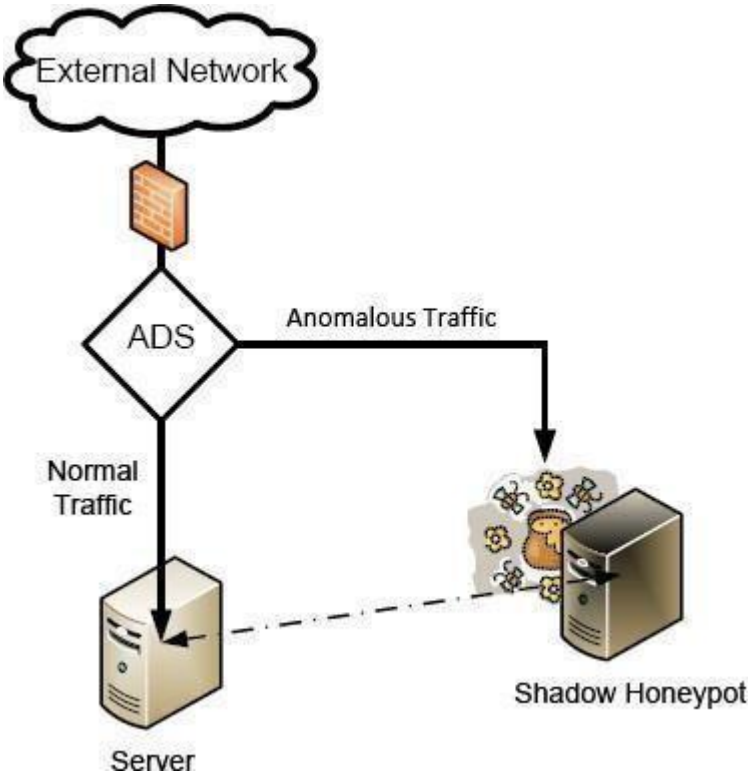


Figure 2. Segmenting traffic in a shadow honeypot system

Distributed Honeypots

One disadvantage of honeypots is that must take up a large portion of the address space in order to be efficient and useful (since attackers and malware must target the honeypots). Yang et al. provide a distributed framework for grid computing in which legitimate hosts redirect suspicious users to a single honeypot . An alternative is used by Honey@home in which each client is responsible for a single unused IP address. The client traffic is redirected anonymously through the Tor network to a collection of central honeypots .

Honeyfarms, honeynets, and distributed honeypots all address the need to monitor a large set of network addresses in order for a honeypot to be effective. As discussed in Section 2.1, grouping honeypots can also add functionality to honeypots by allowing for operations such as simulated outbound traffic. Honeynets, shadow honeypots, and distributed honeynets are just a few of the advances occurring in the field of honeypots. We encourage you to explore journals and online to read about the latest advances.

Existing Honeypot Products

In this section, we provide a very brief survey of the Honeyd, HoneyBOT, and Specter honeypots. For each, we describe what differentiates the solution and provide reference information. We then offer advice for selecting amongst the solutions.

Honeyd

Honeyd is a honeypot for linux/unix developed by security researcher Niels Provos. Honeyd was ground- breaking in that it could create multiple virtual hosts on the network (as opposed to just using a single physical host). The honeypot can emulate various operating systems (which differ in how they respond to certain messages) and services. Since Honeyd emulates operating systems at the TCP/IP stack level, it can fool even sophistic network analysis tools such as nmap. Upon attack, Honeyd can passively attempt to identify the remote host. The Honeyd project is located at http://www.honeyd.org/

HoneyBOT

HoneyBOT is a Windows medium-interaction honeypot by Atomic Software Solutions (http://www.atomicsoftwaresolutions.com/honeybot.php). It originally began as an attempt to detect by the Code Red and Nimda worms in 2001 and has been released for free public use since 2005. HoneyBOT allows attackers to upload files to a quarantined area in order to detect trojans and rootkits. HoneyBOT's user interface is shown in Figure 3.

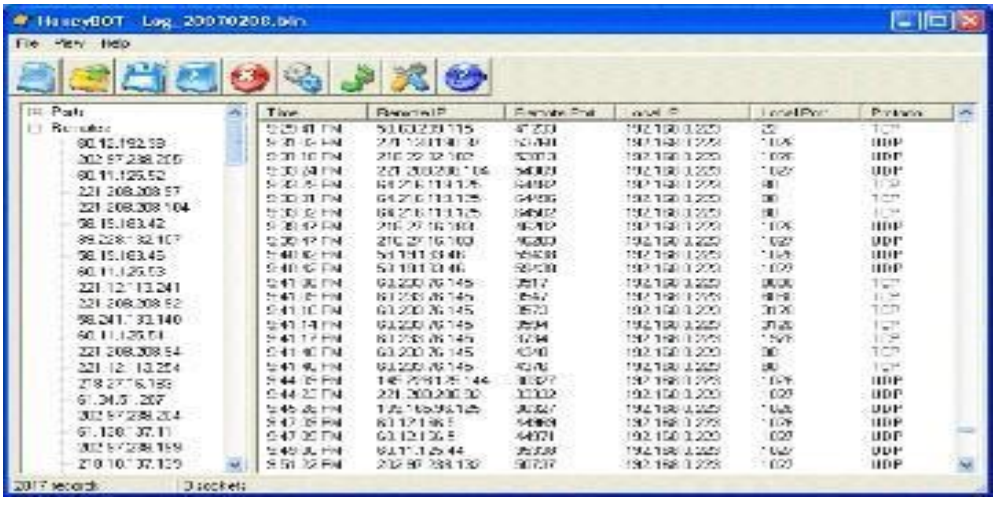


Figure3.The main HoneyBOT user interface.
Taken fromhttp://www.atomicsoftwaresolutions.com/screenshot.php.

Specter

Specter's authors describes Specter as a "honeypot-based intrusion detection system". However, the product is primarily a honeypot designed to lure attackers away from production systems and collect evidence against the attackers. Specter has a few interesting features not found in other solutions:

- Specter makes decoy data available for attackers to access and download. These data files leave marks on the attacker's computer as evidence
- Specter can emulate machines in different states: a badly configured system, a secured system, a failing system (with hardware or software failures), or an unpredictable system.
- Specter actively attempts to collect information about each attacker

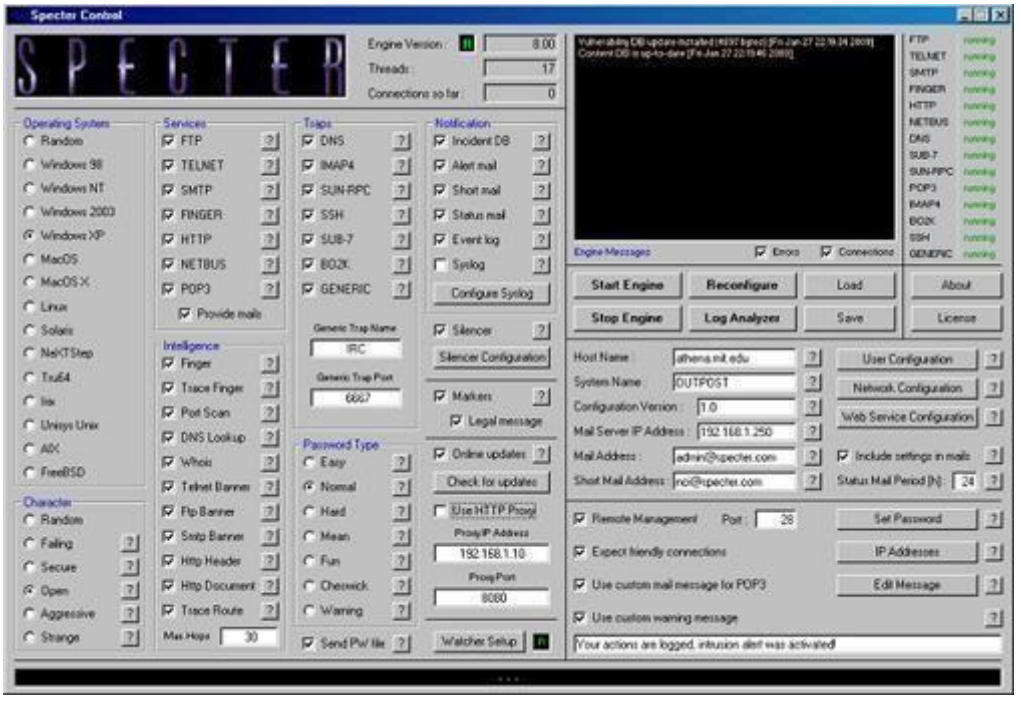


Figure 4. The Specter control center. Taken from http://www.specter.ch/details50.htm.

Conclusion: Hence we have successfully studied honeypot.

Assignment No: 6

Mini–project- Design and develop a tool for digital forensic of images

Link https://www.researchgate.net/publication/337982446_DESIGN_AND_IMPLEMENTATION_OF_DIGITAL_IMAGE_TOOL_FOR_FORENSIC_ANALYSIS_ANALYSIS

Content Of Report:

- **Abstract**
- **Introduction**
- **Methodology**
- **System Requirements**
- **Hardware Requirement**
- **Software Requirements**
- **Conclusion**
- **References**

Assignment No: 7

Title: TEST Scenario

Problem statement: Write TEST Scenario for Gmail Login Page.

Objectives:

To Write TEST Scenario for Gmail Login Page.

Theory:

Test Cases of a Login Page (Test Scenarios Login Page):

Following are the test cases for User Login Page. The list consists of both Positive and Negative test scenarios of login page along with UI test cases, Security test cases and so on.

UI Test Scenarios of Login Page

1. Verify that the login screen contains elements such as Username, Password, Sign in button, Remember password check box, Forgot password link, and create an account link.
2. Verify that all the fields such as Username, Password has a valid placeholder
3. Verify whether all the text boxes have a minimum and maximum length.
4. Verify that the labels float upward when the text field is in focus or filled (In case of the floating label).
5. Verify to see if the font style and size of the labels, as well as the text on each object, are clearly visible.
6. Verify that the application's user interface (UI) is responsive, so it will adapt to different screen resolutions and devices.
7. Verify the login page and all the fields in the login page are displaying without any break in different browsers.

Functional Test Scenarios of Login Page

1. Verify that cursor is focused on the ―Username‖ text box on the page load (login page)
2. Verify that tab functionality is working properly or not
3. Verify that Enter/Tab key works as a substitute for the Sign-in button
4. Verify that the User is able to Login with Valid Credentials
5. Verify that the User is not able to Login with an invalid Username and invalid Password
6. Verify that the User is not able to Login with a Valid Username and invalid Password
7. Verify that the User is not able to log in with an invalid Username and Valid Password
8. Verify that the User is not able to log in with a blank Username or Password
9. Verify that the User is not able to Login with inactive credentials
10. Verify that the reset button clears the data from all the text boxes in the login form
11. Verify that the login credentials, mainly password stores in a database in an encrypted format

12. Verify that clicking on the browser back button after successful login should not take the User to log out mode.
13. Verify that validation message is displayed in the case when User leaves Username or Password as blank
14. Verify that validation message is displayed in case of exceeding the character limit of the Username and Password fields
15. Verify that validation message is displayed in case of entering special character in the Username and password fields
16. Verify that the ―Keep me logged in‖ checkbox is unselected by default (depends on business logic, it may be selected or unselected)
17. Verify that the timeout of the login session (Session Timeout)
18. Verify that the logout link is redirected to login/home page
19. Verify that User is redirected to appropriate page after successful login
20. Verify that the User is redirected to the Forgot password page when clicking on the Forgot Password link
21. Verify that the User is redirected to the Create an account page when clicking on the Signup / Create an account link
22. Verify that the User should be able to login with the new password after changing the password
23. Verify that the user should not be able to login with the old password after changing the password
24. Verify that spaces should not be allowed before any password characters attempted
25. Verify whether the user is still logged in after a series of actions such as sign-in, close the browser, and reopen the application.
26. Verify that the ways to retrieve the password if the user forgets the password

Non-functional Security Test Cases for Login Page

1. Verify that clicking on the browser back button after successful logout should not take the User to a logged-in mode
2. Verify that there is a limit on the total number of unsuccessful login attempts (No. of invalid attempts should be based on business logic. Based on the business logic, User will be asked to enter the captcha and try again or user will be blocked)
3. Verify that the password is in encrypted form (masked format) when entered in the password field.
4. Verify the password can be copy-pasted. System shouldn‘t allow users to copy paste password.
5. Verify that encrypted characters in the ―Password‖ field should not allow deciphering if copied
6. Verify that the ―Remember password‖ checkbox is unselected by default (depends on business logic, it may be selected or unselected).

7. Verify whether the login form is revealing any security information by viewing the page source
8. Verify that the login page is vulnerable to SQL injection.
9. Verify whether Cross-site scripting (XSS) vulnerability works on a login page. XSS vulnerability may be used by hackers to bypass access controls.

Performance Test Cases for Login Page

Verify that how much time the application is taking to load the home page after entering the valid user name and password in the login page.

Test Cases for CAPTCHA & Cookies (If there is a captcha on the login page)

1. Verify that whether there is a client-side validation when the User doesn‘t enter the CAPTCHA
2. Verify that the refresh link of CAPTCHA is generating the new CAPTCHA
3. Verify that the CAPTCHA is case sensitive
4. Verify whether the CAPTCHA has audio support to listen
5. Verify whether virtual keyboard is available and working properly to enter login credentials incase of banking applications.
6. Verify two-way authentication through OTP is working properly incase of banking applications.
7. Verify SSL certificate is implemented or not
8. Verify that the user is able to login when the browser cookies are cleared. When the cookies are cleared, system should not allow user to login automatically.
9. Verify the login functionality when the browser cookies are turned off.

Conclusion: Hence We have learned to write the test cases for Gmail login page.

Assignment No:8

Title:- Test cases

Problem statement:-
Write Test cases in excel sheet for Social Media application or website .

Objectives:
To Write Test cases in excel sheet for Social Media application or website .

Theory:

What are Test Cases?

A test case is a test scenario to test functionality with a different set of input and parameters. We test the expected Result of the test case with the expected one. The test case is marked as passed if the output matches and is marked as failed if the output of expected and doesn‘t match. Test cases can be executed manually or via automation.

Test cases are maintained in test management tools like Jira, HP QC, and others. Let‘s look at the main components of test cases.

- Test Case ID
- Test Case Description
- Assumptions
- Test Data
- Pre-Condition
- Test Steps
- Expected Test Result
- Actual Test Result
- Status Pass/Fail
- Comments

Types of Test Cases

There are different test cases based on the testing methodologies you are following in your project. Some are Functional, API, Performance, Security, Usability, UI, Database, and Unit Test Cases. Functional Test Cases are the ones that are written to test every functionality of the application against user requirements defined by stakeholders. API Test Cases are the ones that are executed before UI is developed for functionality. We test various APIs against different sets of inputs and conditions. Performance and Security Test cases are used to test the application‘s load capacity and vulnerabilities, respectively.

Usability Test Cases are executed to evaluate how user-friendly is our application. Database test cases are mostly SQL or No SQL-based testing. Unit test cases are written by developers to test their code effectively.

How to Write Test Cases in an Excel Sheet

For writing test cases in excel you need to make an excel sheet. There is no specific template for writing test cases that have 10 different columns – Test Case ID, Test Case Description, Assumptions, Test Data, Pre-Condition, Test Steps, Expected Result, Actual Result, Status, and Comments. Suppose you want to write a test case to test a login functionality.

Test Case ID: Test Case ID will be the test case number of story number in JIRA.

Test Case Description: The description will be a short description of the functionality.

Assumptions: Assumptions should be mentioned in the assumptions columns if any.

Test Data: Test Data is the data with which you are performing the testing.

Pre-condition: Pre-condition should be anything that is done before the execution of the test case.

Test Steps: In Test Steps, you must mention steps like Login to application, Enter Username, and password, click the login button, Verify the page redirects to splash page.

Expected Result: The expected Result should indicate the behavior of the application after the execution of the test case. For successful Login expected Result would be a redirection to the splash page.

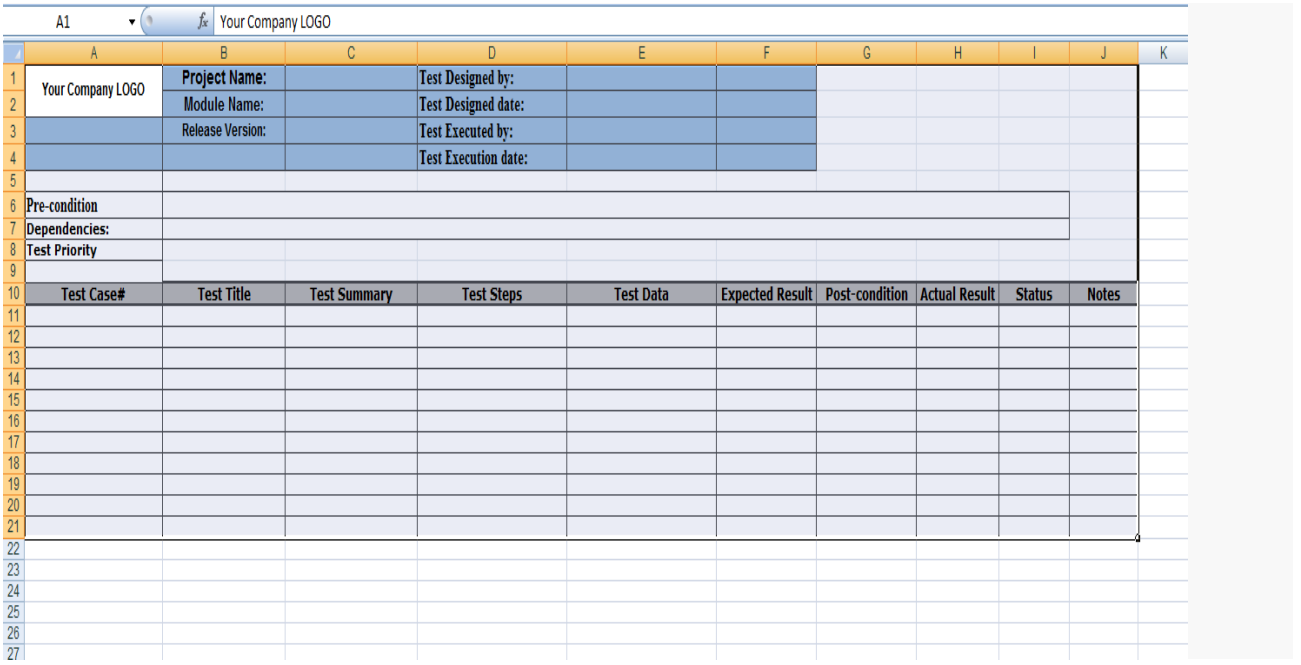
Actual Result: The actual Result indicates the actual behaviour of the application on the execution of the test case.

Status: Status can be marked as passed or fail depending on the actual Result.

Comments: Last is the optional comments.

Example

- Link : https://www.softwaretestinghelp.com/test-case-template-examples/



	A	B	C	D	E	F	G	H	I	J	K
1	Your Company LOGO	Project Name:		Test Designed by:							
2		Module Name:		Test Designed date:							
3		Release Version:		Test Executed by:							
4				Test Execution date:							
5											
6	Pre-condition										
7	Dependencies:										
8	Test Priority										
9											
10	Test Case#	Test Title	Test Summary	Test Steps	Test Data	Expected Result	Post-condition	Actual Result	Status	Notes	
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											
27											

Below are the Test Cases for the same:

Test Scenario ID	Login-1	Test Case ID	Login-1A
Test Case Description	Login – Positive test case	Test Priority	High
Pre-Requisite	A valid user account	Post-Requisite	NA

Test Execution Steps:

S.No	Action	Inputs	Expected Output	Actual Output	Test Browser	Test Result	Test Comments
1	Launch application	https://www.facebook.com/	Facebook home	Facebook home	IE-11	Pass	[Priya 10/17/2017 11:44 AM]: Launch successful
2	Enter correct Email & Password and hit login button	Email id : test@xyz.com Password: ******	Login success	Login success	IE-11	Pass	[Priya 10/17/2017 11:45 AM]: Login successful

Test Scenario ID	Login-1	Test Case ID	Login-1B
Test Case Description	Login – Negative test case	Test Priority	High
Pre-Requisite	NA	Post-Requisite	NA

Test Execution Steps:

S.No	Action	Inputs	Expected Output	Actual Output	Test Browser	Test Result	Test Comments
1	Launch application	https://www.facebook.com/	Facebook home	Facebook home	IE-11	Pass	[Priya 10/17/2017 11:44 AM]: Launch successful
2	Enter invalid Email & any Password and hit login button	Email id : invalid@xyz.com Password: ******	The email address or phone number that you've entered doesn't match any account. Sign up for an account.	The email address or phone number that you've entered doesn't match any account. Sign up for an account.	IE-11	Pass	[Priya 10/17/2017 11:45 AM]: Invalid login attempt stopped

Conclusion: we have studied how to Write Test cases in excel sheet for Social Media application.

Assignment No:9

Title: Defect Report

Problem statement:- Create Defect Report for bug application

Objectives:

To Create Defect Report for bug application.

Theory:

Qualities of a Good Software Bug Report

Anyone can write a Bug report. But not everyone can write an effective Bug report. You should be able to distinguish between an average bug report and a good bug report.

How to distinguish between a good and bad Bug Report? It‘s very simple, apply the following characteristics and techniques to report a bug.

Characteristics and Techniques

#1) Having a clearly specified Bug Number: Always assign a unique number to each bug report. This, in turn, will help you identify the bug record. If you are using any automated bug-reporting tool then this unique number will be generated automatically each time you report a bug.
Note the number and a brief description of each bug that you reported.

#2) Reproducible: If your bug is not reproducible, then it will never get fixed.
You should clearly mention the steps to reproduce the bug. Do not assume or skip any reproducing steps. The bug which is described Step by step is easy to reproduce and fix.

#3) Be Specific: Do not write an essay about the problem.
Be Specific and to the point. Try to summarize the problem in minimum words yet in an effective way. Do not combine multiple problems even if they seem to be similar. Write different reports for each problem.

How To Report A Bug?

Use the following simple Bug report template:
This is a simple Bug report format. It may vary depending upon the Bug report tool that you are using. If you are writing a bug report manually then some fields need to be mentioned specifically like the Bug number – which should be assigned manually.

Reporter: Your name and email address. **Product:** In which product you found this bug. **Version:** The product version, if any.
Component: These are the major sub-modules of the product.
Platform: Mention the hardware platform where you found this bug. The various platforms like _PC‘, _MAC‘, _HP‘, _Sun‘ etc.

Operating system: Mention all the operating systems where you found the bug. Operating systems like Windows, Linux, Unix, SunOS, and Mac OS. Also, mention the different OS versions like Windows NT, Windows 2000, Windows XP etc, if applicable.
Priority: When should a bug be fixed? Priority is generally set from P1 to P5. P1 as ―fix the bug with the highest priority‖ and P5 as ‖ Fix when time permits‖.
Severity: This describes the impact of the bug.

Types of Severity:

- **Blocker:** No further testing work can be done.
- **Critical:** Application crash, Loss of data.
- **Major:** Major loss of function.
- **Minor:** Minor loss of function.
- **Trivial:** Some UI enhancements.
- **Enhancement:** Request for a new feature or some enhancement in the existing one.

- **Application testing scenario :**
  Lets assume in your application you want to create a new user with his/her information, for that you need to logon into the application and navigate to USERS menu > New User, then enter all the details in the User form like, First Name, Last Name, Age, Address, Phone etc. Once you enter all these need to click on SAVE button in order to save the user and you can see a success message saying, ―New User has been created successfully‖.

  Now you entered into your application by logging in and navigate to USERS menu > New user, entered all the information and clicked on SAVE button and now the application crashed and you cansee one error page on the screen, now you would like to report this BUG.

Now here is how we can report bug for above scenario:

- **Bug Name:** Application crash on clicking the SAVE button while creating a new user. **Bug ID:** The BUG Tracking tool will automatically create it once you save this. **Area Path:** USERS menu > New Users **Build Number:**/Version Number 5.0.1
  Severity: HIGH (High/Medium/Low)
  Priority: HIGH (High/Medium/Low)

- **Assigned By:** Your **to:** Developer-X
  Created Name
  Created On: Date
  Reason: Defect

- **Status:** New/Open/Active – Depends on the Tool you are using
  Environment: Windows 2003/SQL Server 2005

- **Description:**
  Application crash on clicking the SAVE button while creating a new user, hence unable to create a new user in the application.

Steps To Reproduce:

1. Logon into the application
2. Navigate to the Users Menu > New User
3. Filled all the fields
4. Clicked on _Save' button
5. Seen an error page —ORA1090 Exception: Insert values Error…‖
6. See the attached logs for more information
7. And also see the attached screenshot of the error page.

- **Expected:** On clicking SAVE button should be prompted to a success message —New User has been created successfully‖.

- Save the defect/bug in the BUG TRACKING TOOL.

Conclusion: Hence, we have successfully studied concept of how to write defect report for the application.

Assignment No: 10

Title: Selenium gri

Problem Statement: Installation of Selenium grid and selenium Web driver java eclipse (automation tools).

Objectives: To Install Selenium grid and selenium Web driver java eclipse (automation tools).

Theory:

What Is Selenium Grid?

Selenium Grid is a part of the Selenium Suite that specializes in running multiple tests across different browsers, operating systems, and machines in parallel. It is achieved by routing the commands of remote browser instances where a server acts as a hub. A user needs to configure the remote server in order to execute the tests.
Selenium Grid has 2 versions – the older Grid 1 and the newer Grid 2. We will only focus on Grid 2 because Grid 1 is gradually being deprecated by the Selenium Team.

Selenium Grid uses a hub-node concept where you only run the test on a single machine called a **hub**, but the execution will be done by different machines called **nodes**.

When
You sh[illegible] f following:

- **Run your tests against different browsers, operating systems, and machines all at the same time**

  This will ensure that the application you are Testing is fully compatible with a wide range

  of browser-O.S combinations.

- **Save time in the execution of your test suites**.

  If you set up Selenium Grid to run, say, 4 tests at a time, then you would be able to finish the whole suite around 4 times faster.

What Is Selenium WebDriver(Selenium 2.0)?

Selenium WebDriver allowed you to directly interact with the browsers through your automation test scripts. Java, PHP, C#, Python, Ruby, Perl, and Javascript are some of the programming languages it supports.

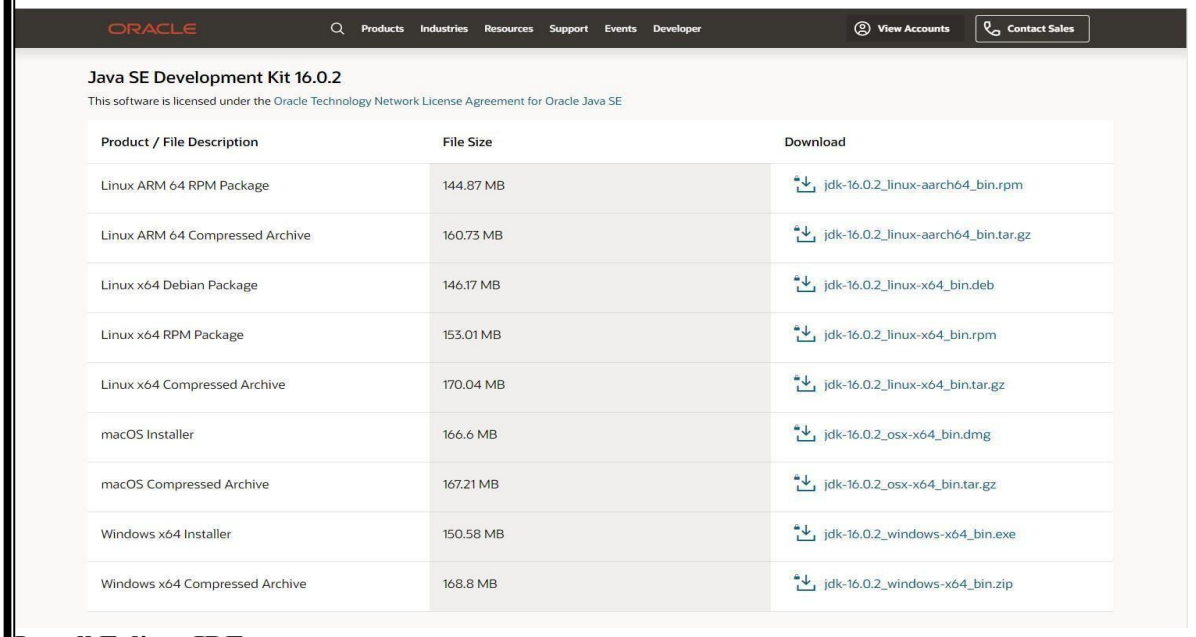
The browsers it supports include Mozilla Firefox, Google Chrome version 12.0.712.0 and above, Internet Explorer, Safari, Opera version 11.5 and above, and HtmlUnit version 2.9 and above.

As for operating systems, Selenium WebDriver supports Windows, Linux, Mac OS, and Solaris. Selenium WebDriver is also known as Selenium 2.

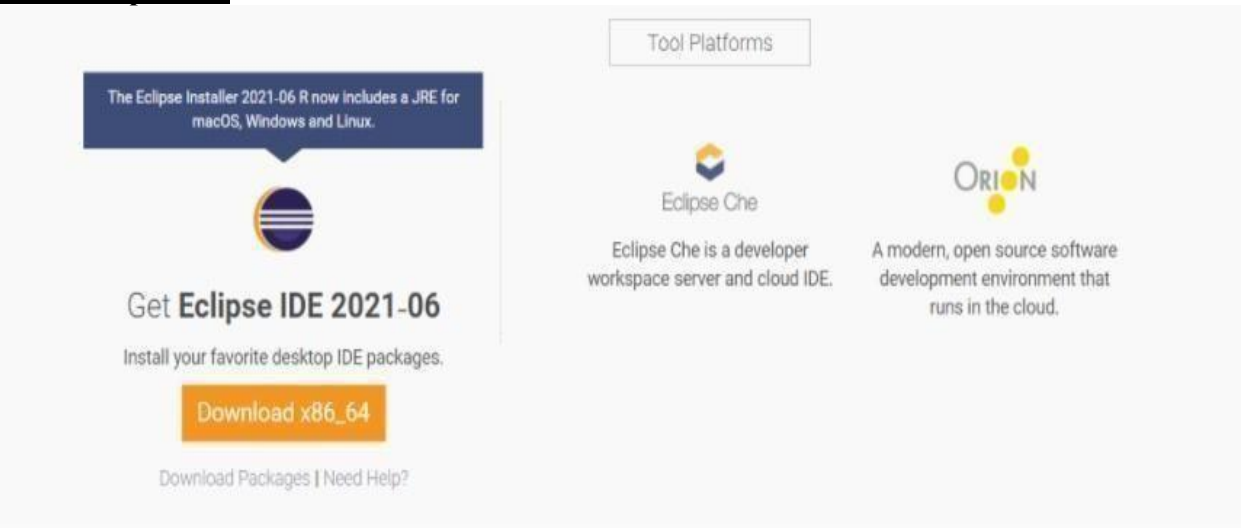
Selenium WebDriver does not handle window component, but this limitation can be overcome by using external tools such as AUTO IT tool, Sikuli etc. It has different location strategies as well such as ID, Name, Link text, Partial link text, Class name, CSS selector and Xpath. It also has better support dynamic web pages like Ajax, where elements of the web page may change without the page itself being reloaded.
By using different jar files, we can also test API, Database Test etc. using Selenium WebDriver.

Link : https://www.browserstack.com/guide/how-to-setup-selenium-in-eclipse

- **Prerequisites for configuring Selenium in Eclipse**
- **Install Java** Download Java SE Development Kit 16.0.2 according to the Windows, Linux,
- Run the JDK Installer by double-clicking on the file name in the download location and following the instructions on the instruction wizard. Alternatively, silently install JDK by entering the following command:
- jdk.exe /s



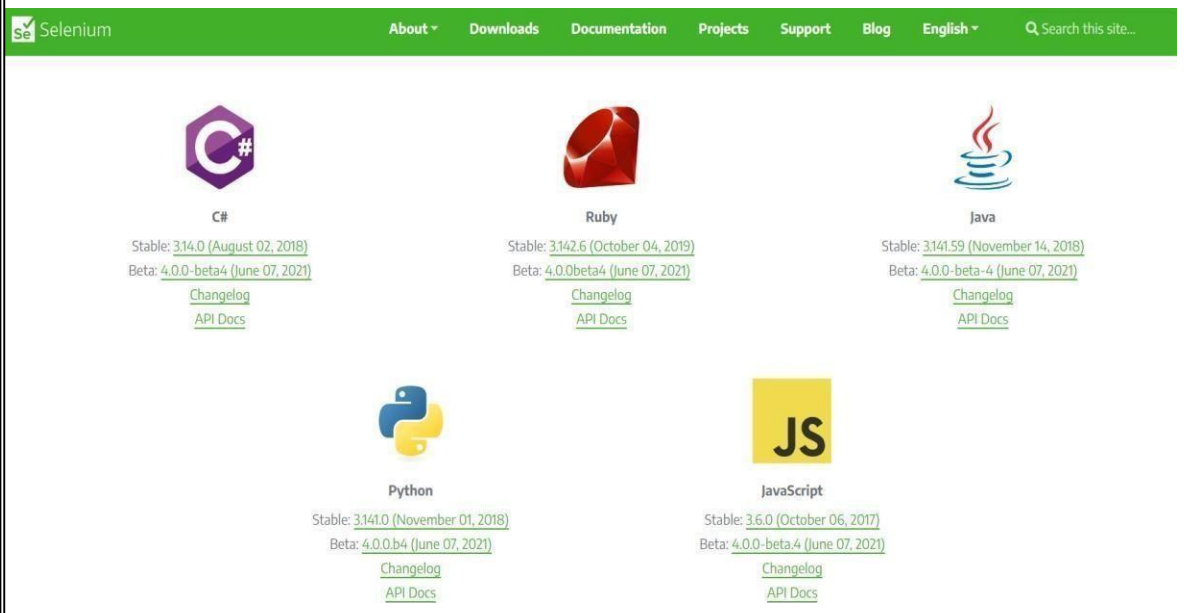
Install Eclipse IDE



Install Selenium

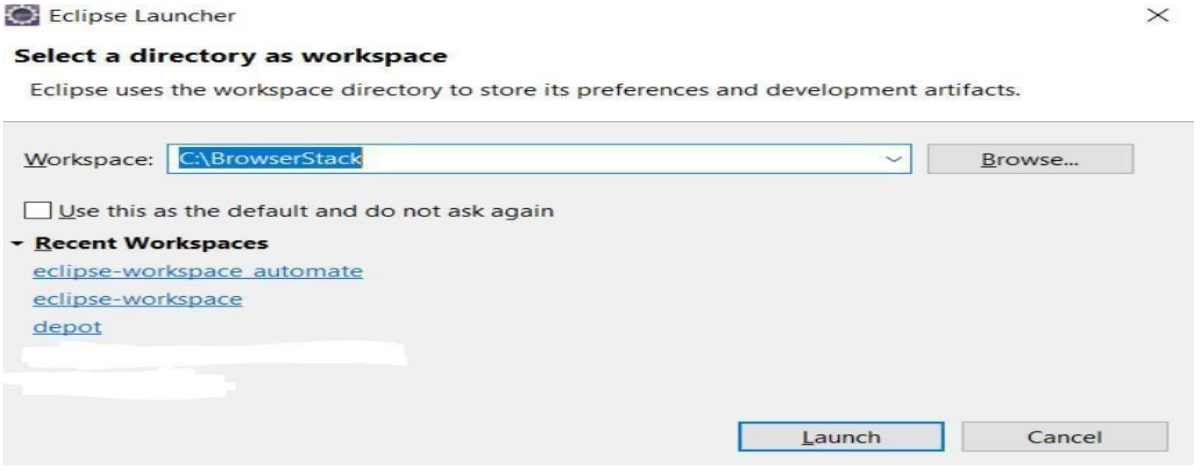
- Download and Install Selenium to be set up in Eclipse.
- **Install Browser Driver**
- For Cross Browser Testing, download the relevant Browser Driver – Chrome Driver (for Chrome),
- Gecko Driver (for Firefox), Safari Driver(for Safari), and Internet Explorer Driver and MS Edge Driver
- IE and Edge respectively
- Place these Browser Driver files in a directory that is part of the environment PATH. This will allow a command-line call to the programs to execute them irrespective of the working directory.
- **Install Java Language Bindings Version 3.141.59 (2018)**

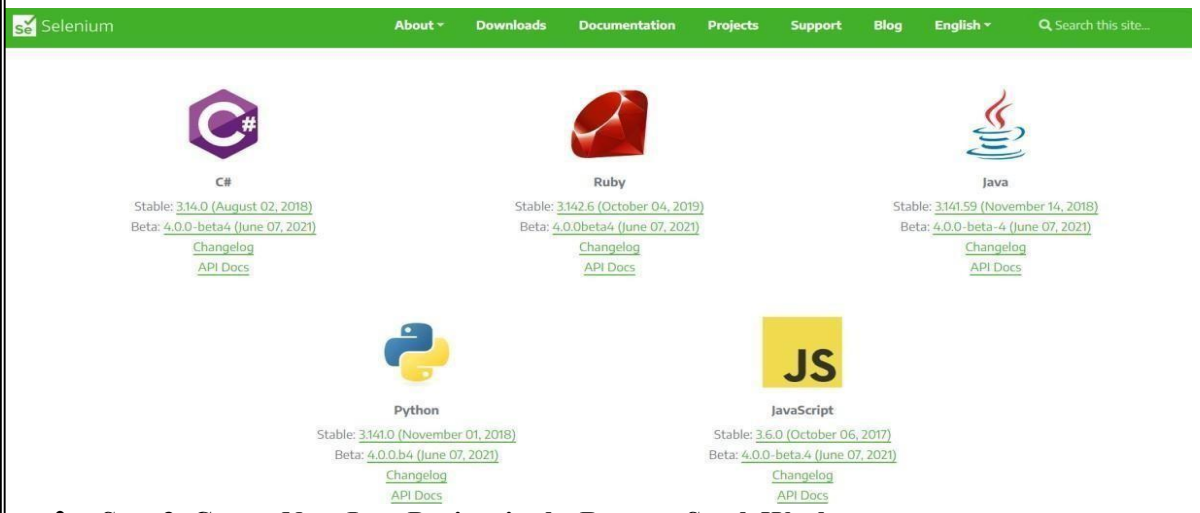
- API Docs



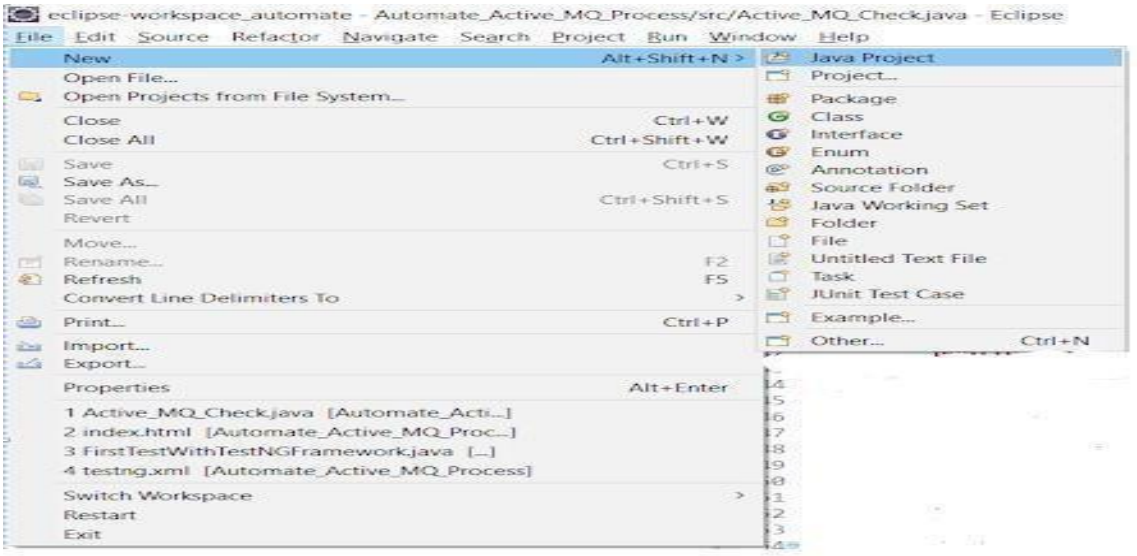
How to configure Selenium in Eclipse

- Here are the steps to configure Selenium Webdriver with Eclipse:
- **Step 1: Launch Eclipse**
- To launch Eclipse double click on the **eclipse.exe** file in the download location.
- **Step 2: Create Workspace in Eclipse**
- This workspace named –**C:\BrowserStack**‖ is like any other folder, which will store all the test scripts.
- Launch the BrowserStack workspace.

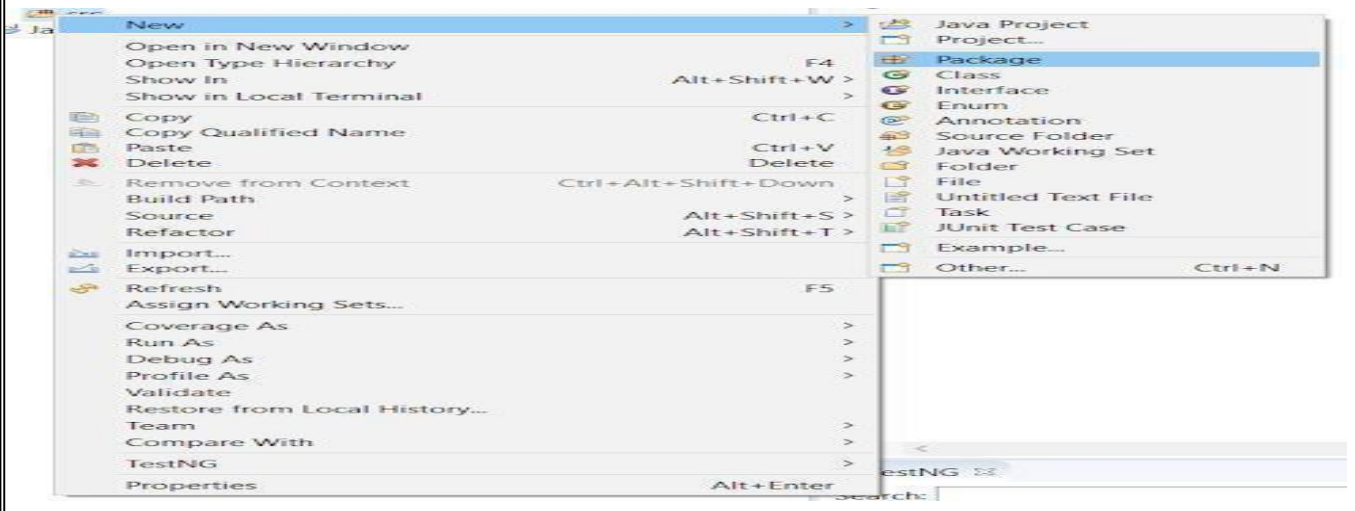




- **Step 3: Create New Java Project in the BrowserStack Workspace**
- Create a new Java Project by clicking on **File > New > Java Project** and name it.



- **Creatinga new Java Project**
  Step 4: Create Package and Class under the Java Project
- By clicking on the **src folder** (which is the source folder), create a new package and name it
- Then right-click on the package name and create a class.



Conclusion: Hence, we have successfully studied Installation of Selenium grid and selenium Web driver java eclipse.

Assignment No: 11

Title: Software requirement specification

Problem Statement: Prepare Software requirement specification for online education portal

Objectives:

To Prepare Software requirement specification for online education portal

Theory:

What Is a Software Requirements Specification (SRS) Document?

A software requirements specification (SRS) is a document that describes what the software will do and how

it will be expected to perform. It also describes the functionality the product needs to fulfill all stakeholders (business, users) needs.

An SRS can be simply summarized into four Ds:

- Define your product's purpose.
- Describe what you're building.
- Detail the requirements.
- Deliver it for approval.

We want to DEFINE the purpose of our product, DESCRIBE what we are building, DETAIL the individual requirements, and DELIVER it for approval. A good SRS document will define everything from how software

will interact when embedded in hardware to the expectations when connected to other software. An even better SRS

documents also account for real-life users and human interaction.

The best SRS documents define how the software will interact when embedded in hardware — or when

connected to other software. Good SRS documents also account for real-life users.

Why Use an SRS Document?

An SRS gives you a complete picture of your entire project. It provides a single source of truth that every team involve in development will follow. It is your plan of action and keeps all your teams — from development to maintenance — o the same page (no pun intended).

make vital decisions on your product‘s lifecycle, such as when to retire an obsolete feature.

The time it takes to write an SRS is given back in the development phase. It allows for better understanding or your product, team, and the time it will take to complete.

Software Requirements Specification vs. System Requirements Specification

A **software requirements specification (SRS)** includes in-depth descriptions of the software that will be developed.

A **system requirements specification (SyRS)** collects information on the requirements for a system. ―Software‖ and ―system‖ are sometimes used interchangeably as SRS. But, a software requirement specification provides greater detail than a system requirements specification.

>> Need to prove compliance? Here's how to create a traceability matrix >>

How to Write an SRS Document

Writing an SRS document is important. But it isn‘t always easy to do. Here are five steps you can follow to write an effective SRS document.

1. Define the Purpose With an Outline (Or Use an SRS Template)

Your first step is to create an outline for your software requirements specification. This may be something you create yourself. Or you may use an existing SRS template. If you‘re creating this yourself, here‘s what your outline might look like:

1. Introduction

- 1.1 Purpose
- 1.2 Intended Audience
- 1.3 Intended Use
- 1.4 Scope
- 1.5 Definitions and Acronyms

2. Overall Description

- 2.1 User Needs
- 2.2 Assumptions and Dependencies

3. System Features and Requirements

- 3.1 Functional Requirements

3.2 External Interface Requirements

3.3 System Features

3.4 Nonfunctional Requirements

This is a basic outline and yours may contain more (or fewer) items. Now that you have an outline, lets fill in the blanks.

Download a white paper on best practices for writing requirements >>

2. Define your Product's Purpose

This introduction is very important as it sets expectations that we will hit throughout the SRS. Some items to keep in mind when defining this purpose include:

Intended Audience and Intended Use

Define who in your organization will have access to the SRS and how they should use it. This may include developers, testers, and project managers. It could also include stakeholders in other departments, including leadership teams, sales, and marketing. Defining this now will lead to less work in the future.

Product Scope

What are the benefits, objectives, and goals we intend to have for this product? This should relate to overall business goals, especially if teams outside of development will have access to the SRS.

Definitions and Acronyms

It's important to define the risks in the project. What could go wrong? How do me mitigate these risks? Who is in charge of these risk items?
For example, if the failure of a medical device would cause slight injury, that is one level of risk.

Taking into account the occurrence level and the severity, we can come up with a strategy to mitigate this risk.

>> Need to create a PRD? Here's a how-to with examples >>

3. Describe What You Will Build

Your next step is to give a description of what you're going to build. Is it a new product? Is it an add-on to a product you've already created? Is this going to integrate with another product? Why is this needed?

Who is it for?

Understanding these questions on the front end makes creating the product much easier for all involved.

User Needs

Describe who will use the product and how. Understanding the user of the product and their needs is a critical part of the process.

Who will be using the product? Are they a primary or secondary user? Do you need to know about the purchaser of the product as well as the end user? In medical devices, you will also need to know the needs of the patient.

Assumptions and Dependencies

What are we assuming will be true? Understating and laying out these assumptions ahead of time will help with headaches later. Are we assuming current technology? Are we basing this on a Windows framework?

We need to take stock of these assumptions to better understand when our product would fail or not operate perfectly.

Finally, you should note if your project is dependent on any external factors. Are we reusing a bit of software from a previous project? This new project would then depend on that operating correctly and should be included.

4. Detail Your Specific Requirements

In order for your development team to meet the requirements properly, we MUST include as much detail as possible. This can feel overwhelming but becomes easier as you break down your requirements into categories.

Some common categories are:

Functional Requirements

Functional requirements are essential to your product because, as they state, they provide some sort of functionality. Asking yourself the question ―does this add to my tool‘s functionality?‖ Or ―What function does this provide?‖ can help with this process. Within Medical devices especially, these functional requirements may have a subset of risks and requirements.

You may also have requirements that outline how your software will interact with other tools, which brings us to external interface requirements.

External Interface Requirements

External interface requirements are specific types of functional requirements. These are especially important when working with embedded systems. They outline how your product will interface with other components.

There are several types of interfaces you may have requirements for, including:

- User
- Hardware
- Software
- Communications

System Features

System features are types of functional requirements. These are features that are required in order for a system to function.

Other Nonfunctional Requirements

Nonfunctional requirements can be just as important as functional ones. These include:

- Performance
- Safety
- Security
- Quality

The importance of this type of requirement may vary depending on your industry.

In the medical device industry, there are often regulations that require the tracking and accounting of safety. IEEE also provides guidance for writing software requirements specifications, if you're a member.

5. Deliver for Approval

We made it! After completing the SRS, you'll need to get it approved by key stakeholders. This will require everyone to review the latest version of the document.

Link : https://impressit.io/blog/software-requirements-specification-guide

Brief Requirements Specification: Online Education Portal

Background: I own an expanding UK-based company which provides online English teaching services to companies and individuals in Russia.

Objective: To hire and properly monitor a team of English teachers in the UK, ensure student/teacher loyalty and cope with an expanding client base.

Maximum Load: 20 teachers, 200 students, 10 classes conducted simultaneously.

Current website: www.englishinrussia.ru

Site concept: Online education portal for Russian learners of English.

Competitors: http://www.englishdom.com, http://www.english-natali.ru

Features to be added:

1) **Stand-alone server software** in addition to the existing webserver.
   - Platform is subject to discussion
   - Its URL can be different from main website
   - Russian language support is a must
   - Database
2) **On-site web-conferencing system** similar to Skype, but simpler. This is an essential element of the site to guarantee control of the teaching process and to maintain teacher/student loyalty.
   - Ability to save information about classes: teacher, student, topic, start/end date and time, mark, comment
   - Two-way video stream
   - Quality audio
   - Text chat
   - Screen share
   - Whiteboard functionality
   - Option of recording lessons
3) **Back office for registered students.**
   - Login
   - Real-time updated student timetables
   - Teacher availability timetables
   - Payment system
   - Lesson booking and links to payment system
   - Teacher profiles with samples from lessons (embedded video, audio)
   - Internal messaging system for sending homework and questions/answers between students and teachers with the option of attaching files.
4) **Payment system.** Payment for lessons and courses online (similar to this: http://www.englishdom.com/en/cost).
5) **Online test functionality.** Interactive exercises in the form of multiple choice questions (similar to this: http://cliomsk.com/on-line-test). This should be created as a customisable template, which can be used to create other interactive exercises by study topic.
6) **Reports.**
   - Ability to monitor who is currently online, who is in the virtual classrooms.
   - Recorded lessons with start date/time and duration
   - Payments list within a selected period, teacher or student.
   - Teacher workload statistics for every teacher
   - Report on student: classes with marks
   - Online test results.
   - Message logs.
   - System log.
7) **Configuration.**
   - User page
   - Student profiles
   - Teacher profiles
   - Online test templates
   - Hourly rates for every teacher

Assignment No: 12

Mini Project :Software Testing and Quality Assurance Mini Project Dynamic website of covid-19 informationusing HTML, CSS, JAVASCRIPT And PHP, MySQL database used to store user account, comment, and registration form details. Regular Expression test cases for testing purpose

Link : https://phpgurukul.com/covid19-testing-management-system-using-php-and-mysql/

- **How to run the Online COVID Testing Management System Using PHP and MySQL**
- Download the zip file
- Extract the file and copy covid-tms folder
- Paste inside root directory(for xampp xampp/htdocs, for wamp wamp/www, for lamp var/www/html)
- Open PHPMyAdmin (http://localhost/phpmyadmin)
- Create a database with name covidtmsdb
- Import covidtmsdb.sql file(given inside the zip package in SQL file folder)
- Run the script http://localhost/covid-tms
- **Admin**

  Credentil
  Username:admin
  Password:Test@123