**Tools to be used for testing the website**

**Kali Linux**

This is a popular Linux operating system well known for penetration testing. It is used to run information security tests to detect and fix vulnerabilities of the website.

**Network testing tools**

This are cloud-based network. They help to find Cybersecurity weakness in the website hence avoiding high costs of data breaches.

**Domain testing tools i.e whois,nslookup**

These tools will be used for tracking the attackers when trying to find targets they want to attack on the website. They return the IP address of the server.

**Port scanning tools**

These tools detect targets with unused ports which are open

**Traffic capture tools (Wireshark)**

These tools intercept data being transferred in a network and capture it, it can be stored analyzed and downloaded.

**Vulnerability assessment tools**

They are used to systematically scan the website and address potential vulnerabilities. This assessments prevent the possibility of unauthorized system access.

**Business impacts on use of tools and methods**

**Cost-effectiveness-** Use of tools in website testing saves a lot of cost as compared to manual testing.

**Time-saving-** Using the tools selected is faster and saves a lot of time which would be used when using local infrastructure.

**Efficient –** It’s efficient to use the tools for better productivity.

**Timeline of the completion of the task.**

The task will be completed in four weeks as scheduled below:

Planning – 1 week (Gathering all resources to be used)

Execution - 2 weeks (Actual testing in all scope targets)

Analysis and Documentation - 1 week (Preparing a summary report of the findings.)

**Limitation and assumptions**

Limitation of scope – Testing a website is not done on the whole website but only selected parts.

Limitation of access – Testers are not allowed to access the whole website when testing.

Limited skills of penetration tester s– Testers mostly have more knowledge in some areas than others.

Its assumed that the tools used are correct and produce sure results thus it gives false sense of producing quality results.

**Impacts on normal operations caused by using the tools**

* Slows down the speed of the site.
* Security matters which can arise on sharing confidential data.

**REFERENCES.**

A study on penetration testing and tools *HMZ AI Shebli,BD Beheshti – 2018 IEEE*

Detecting vulnerabilities in web applications using automated blackbox and penetration testing *NF Awang, A Abd Manaf 2012*

A study of penetration testing tools and approaches *TP Chiem – 2014 – openrepository.aut.ac.nz*