**Vulnerability Assessment and Penetration Testing**

**A Minor Project Report Submitted to**



**Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal**

**Towards Partial Fulfillment for the Award of**

**Bachelor of Technology**

**(Computer Science and Engineering)**

**Submitted By:**

**Siddharth Jain(0827CS171211)**

**Shubham Malviya(0827CS171208)**

**Siddharth Choudhary (0827CS171210)**

**CS4 III YEAR**

**Supervised By: Guided by:**

**Mr. Ritesh Khedekar Mrs. Vandana Kate Ms. Nupur Agrawal**

****

**Department of Computer Science and Engineering**

**Acropolis Institute of Technology and Research, Indore**

**July - Dec 2019**

**REQUIREMENTS DOCUMENT**

**THE KEY PLAYERS**

Before we jump into the 10 types of requirements documents, let's talk about the main people involved in their creation.

* **The Customer** is ultimately responsible for determining the requirements. The customers’ needs are the origin of the project.
* **The Business Analyst** is responsible for *discovering*the problem/requirements and determining the solution.
* **The Project Manager** is responsible for *delivering*the solution to a problem.
* **The Systems Analyst** uses analysis and design to satisfy business requirements using information technology.
* **The Marketing Manager** develops the marketing strategy for the project in line with its requirements.
* **The Product Manager** is responsible for defining the why, when, and what of the product that the development team will build.

**HERE ARE 4 DIFFERENT TYPES OF REQUIREMENTS DOCUMENTS**

**1. Business Requirements Document (BRD)**

A **Business Requirement Document (BRD)** focuses on the business perspective as it holds the details of the business solution for a project. Business requirements document also emphasizes on the needs and expectations of the customer. In simpler terms, BRD indicates what the business wants to achieve.  The BRD indicates all the project deliverable and the inputs and outputs associated with each process function.

The process function is responsible for Critical to Quality (CTQs) parameters that relate to needs and wants of the customer. CTQs are responsible for a positive Voice of Customers (VOC). VOC describes the customer’s feedback about their experiences with your products or services. BRD focuses on the business objectives and distinguishes between the business solution and technical solution.

**Objectives of a business requirement document:**

* To get an agreement among stakeholders
* Communicate to the technology server provider, the business needs, the customer needs, and what the solution needs to do to satisfy business and customer needs
* To determine the input to the next phase of the project
* Describe in details of the needs of the customer and business that the solution intends to meet.

**Key elements**

A[business analyst](https://reqtest.com/requirements-blog/requirements-review-from-ba-perspective/) or a project manager who has a thorough understanding of the [business processes](https://en.wikipedia.org/wiki/Business_process) drafts business requirement document. The business requirement document is drafted for a project to ensure the implementation of all the requirements to achieve business objectives.

The most critical component of a business requirement document is the scope of the project along with the restrictions and constraints. The scope comprises of three key things:

* **What are the problems which the business wants to solve?**

The evolving tools, tactics and procedures used by cybercriminals to breach networks means that it’s important to regularly test your organisation’s cyber security.VAPT helps to protect your organisation by providing visibility of security weaknesses and guidance to address them. VAPT is increasingly important for organisations wanting to achieve compliance with standards including the [GDPR](https://www.redscan.com/services/gdpr/), ISO 27001 and [PCI DSS](https://www.redscan.com/services/pci-dss/).

* **What are the restrictions?**

Following are the major limitations of Penetration Testing –

**Limitation of Time** − As all of us know, penetration testing is not at all time bound exercise; nevertheless, experts of penetration testing have allotted a fixed amount of time for each test. On the other hand, attackers have no time constrains, they plan it in a week, month, or even years.

**Limitation of Scope** − Many of the organizations do not test everything, because of their own limitations, including resource constraints, security constraints, budget constraints, etc. Likewise, a tester has limited scope and he has to leave many parts of the systems that might be much more vulnerable and can be a perfect niche for the attacker.

**Limitation on Access** − More often testers have restricted access to the target environment. For example, if a company has carried out the penetration test against its DMZ systems from all across its internet networks, but what if the attackers attack through the normal internet gateway.

**Limitation of Methods** − There are chances that the target system can crash during a penetration test, so some of the particular attack methods would likely be turned off the table for a professional penetration tester. For example, producing a denial of service flood to divert a system or network administrator from another attack method, usually an ideal tactic for a really bad guy, but it is likely to fall outside of the rules of engagement for most of the professional penetration testers.

**Limitation of Skill-sets of a Penetration Tester** − Usually, professional penetration testers are limited as they have limited skills irrespective of their expertise and past experience. Most of them are focused on a particular technology and having rare knowledge of other fields.

**Limitation of Known Exploits** − Many of the testers are aware with only those exploits, which are public. In fact, their imaginative power is not as developed as attackers. Attackers normally think much beyond a tester’s thinking and discover the flaw to attack.

**Limitation to Experiment** − Most of the testers are time bound and follow the instructions already given to them by their organization or seniors. They do not try something new. They do not think beyond the given instructions. On the other hand, attackers are free to think, to experiment, and to create some new path to attack.

* **Is it worth to invest the time and money required for the project?**

The need for VAPT is increased because all the IT sector offices needed to ensure the security of data from the increasing threat of hackers. Be it a big enterprise or a medium one, every business that depends heavily on computers and is involved in the big data ecosystem needs to maintain the security of their computer and this is where they make use of VAPT Companies.

VAPT prepares you from real line threats and ensures the safety of your data. There might not be any direct returns by investing in something like them but with time all money spent on security becomes worth every penny. It is better to be safe than sorry. The money that is spent on conducting these tests and assessment is lesser than the money that goes in recovering from hacking attempt.

## An ideal BRD template

The ideal [business requirement document template](https://reqtest.com/requirements-blog/requirements-document-template/) should have the following components:

### A summary statement

Vulnerability Assessment and Penetration Testing (VAPT) are the security services that emphasis on identifying vulnerabilities in the network, server, web application and system infrastructure. Both the services serves a different purpose and are carried out to accomplish diverse however complimentary objectives.

### Project objectives

### The main purpose of the pen test is to improve network security and provide protection for the entire network and connected devices against future attacks. Penetration testing helps to identify vulnerabilities within a network.

### Needs statement

### To keep the financial data secure while transferring it between systems or over networks. To identify security vulnerabilities within an application. To find out loopholes within the system. To assess the tolerance of business in cyber attacks.

### Project scope

**Identifying gaps in security:** Organization can identify the gap of the system security and company can develop an action plan to reduce the threat with the help of penetration test.[Find out more](https://www.ukessays.com/services/essays.php)

**Help to create strong business case:** A penetration test result document will help the manager to create a strong business case to produce the security message at the implementation stage.

**To discover new threats:** Penetration testing measures will help the organization to find the new threats.

**To focus on internal security resources:** A Penetration test and its security analysis allow the organization to focus internal security resources.

**To meet regulatory compliances:** Organization can meet their regulatory compliances using penetration testing tools.

**To find weakest link:** Penetration test and security audit will assist the firm to find the weakest link in their intricate structure and it will provide baseline security for all typical entities.

**Provide validation feedback:** Penetration test deliver validation feedback to business entities and security framework that lead the organization to reduce the risk in the implementation.

### Cost & Benefit

An **average cost of a penetration test** can vary from $4,000 to $100,000. When done correctly, it’s worth every penny. Mainly, because you are getting a specialist or a team of specialists who will work on finding any possible way your system can be affected. Later, you receive a recommendation regarding the discovered vulnerabilities and, when necessary, continuous system support. Another factor that affects **penetration testing costs** is the regularity with which you perform it. As many other assessments, pen tests are necessary on a regular basis, to ensure you comply with all the standards and no new issues appear. Depending on the complexity of your system and the frequency of updates, the recommended testing regularity is once or twice per year..

**2. Functional Requirements Document (FRD)**

The Functional Requirements Document (FRD) is a formal statement of an application’s functional requirements. It serves the same purpose as a contract. Here, the developers agree to provide the capabilities specified. The client agrees to find the product satisfactory if it provides the capabilities specified in the FRD.

Functional requirements capture the intended behavior of the system. This behavior may be expressed as services, tasks or functions the system is required to perform. The document should be tailored to fit a particular project’s need. They define things such as system calculations, data manipulation and processing, user interface and interaction with the application.

The Functional Requirements Document (FRD) has the following characteristics −

* It demonstrates that the application provides value in terms of the business objectives and business processes in the next few years.
* It contains a complete set of requirements for the application. It leaves no room for anyone to assume anything which is not stated in the FRD.
* It is solution independent. The ERD is a statement of what the application is to do— not of how it works. The FRD does not commit the developers to a design. For that reason, any reference to the use of a specific technology is entirely inappropriate in an FRD.

The functional requirement should include the following −

* Descriptions of **data** to be entered into the system

**VAPT** is a term used to describe security testing that is designed to identify and help address cyber security vulnerabilities. **VAPT** could include anything from automated vulnerability assessments to human-led penetration testing and red team operations.

* Descriptions of **operations** performed by each screen

1. BurpSuite **(PT)L**: **Burp** or **Burp Suite** is a graphical tool for testing Web application security. The tool is written in Java and developed by PortSwigger Web Security.

The company behind **Burp Suite** has also developed a mobile application containing similar tools compatible with iOS 8 and above.

1. **Metasploit(PT):** **Metasploit** is an exploit development framework that facilitates penetration testing of IT systems. This tool initially started off as a game and was taken over by Rapid 7 for maintenance and further development.
2. **Sublist3r** : **Sublist3r** is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting.
3. **Nmap** : **Nmap** (Network Mapper) is a free and open-source network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). **Nmap** is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
4. **Dirsearch** is a Python-based command-line website directory scanner designed to brute force site structure including directories and files in websites.
5. **Sqlmap** is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.

* Descriptions of **work-flows** performed by the system

## The life cycles of Vulnerability Assessment and Penetration Testing:

1. Scoping
2. Information gathering
3. Vulnerability scanning
4. False positive analysis
5. Vulnerability exploitation (Penetration Testing)
6. Report generation

The following figure illustrates the different sequential stages recommended to follow for a Vulnerability Assessment or Penetration testing-:

**Stage 1 – Scoping**

Scoping is the primary step of any security assessment activity. In order to execute a VA or PenTest, the first step is to identify the scope of the assessment in terms of infrastructure against which the assessment is to be conducted, for example, servers, network devices, security devices, databases, and applications.

Scoping depends on the business objective of the Vulnerability Assessment. During the scoping, a scanning window should also be agreed upon. Also, the types of attacks that are permitted should be agreed upon. After deciding on the scope of assessment, this phase also includes planning and preparation for the test, which includes deciding on the team, date, and time of the test.

Another major factor that should be taken care of prior to beginning the engagement is signing a formal engagement agreement between the security tester and the party on whose infrastructure these tests will be performed.

Scoping should also include identifying the count of infrastructure elements to be tested.

Apart from the infrastructure scope and other program management modalities, the exact scope, the organization’s approach to the business objective, and the methodology of the assessment should be decided. For deciding on the business objective, the organization should identify the type of attack that it would like to get mimicked.

An example of an objective that a company might seek is: “To find out what an external attacker can achieve by targeting externally exposed infrastructure with only the knowledge of a publicly exposed IP address.” This type of requirement will be met through an external Black box penetration testing of infrastructure and applications, and the approach and the methodology should be in accordance with that.Based on the accessibility of infrastructure from the Internet or intranet, the testing can be done from an external or internal network. Also, based on the type of details, the infrastructure testing can be Black box or Grey box. And depending on the type of infrastructure, the plugins or features of a vulnerability scanning tool should be enabled, aided by appropriate manual checks.

## Stage 2 – Information gathering

Information gathering is the second and most important stage of a VA-PT assessment. This stage includes finding out information about the target system using both technical (WhoIS) and nontechnical passive methods such as the search engine.

This step is critical as it helps in getting a better picture of the target infrastructure and its resources. As the timeline of the assessment is generally time bound, information captured during this phase helps in streamlining the effort of testing in the right direction by using the right tools and approach applicable to target systems.

This step becomes more important for a Black box assessment where very limited information about the target system is shared. Information gathering is followed by a more technical approach to map the target network using utilities such as pings and Telnet and using port scanners such as NMAP. The use of such tools would enable assessors to find a live host, open services, operating systems, and other information.

The information gathered through network mapping will further validate information gathered through other passive means about the target infrastructure, which is important to configure the vulnerability scanning tool. This ensures that scanning is done more appropriately.

## Stage 3 – Vulnerability scanning

This stage involves the actual scanning of the target infrastructure to identify existing vulnerabilities of the system. This is done using vulnerability scanners such as Nessus. Prior to scanning, the tool should be configured optimally as per the target infrastructure information captured during the initial phases.

Care should also be taken that the tool is able to reach the target infrastructure by allowing access through relevant intermediate systems such as firewalls.

Such scanners perform protocol TCP, UDP, and ICMP scans to find open ports and services running on the target machine and match them to well- known published vulnerabilities updated regularly in the tool’s signature database if they exist in the target infrastructure. The output of this phase gives an overall view of what kind of vulnerabilities exist in the target infrastructure that if exploited can lead to system compromise.

## Stage 4 – False positive analysis

As an output of the scanning phase, one would obtain a list of vulnerabilities of the target infrastructure. One of the key activities to be performed with the output would be false positive analysis, that is, removing any vulnerability that is falsely reported by the tool and does not exist in reality. All scanning tools are prone to report false positives, and this analysis can be done using methods such as correlating vulnerabilities with each other and previously gathered information and scan reports, along with actually checking whether system access is available.

Vulnerability scanners give their own risk rating to the identified vulnerabilities; these can be revisited considering the actual criticality of the infrastructure element

(server or network device) to the network and impact of the vulnerability.

## Stage 5 – Vulnerability exploitation (Penetration Testing)

In case system owners require proof of existing vulnerabilities or exploits to understand the extent to which an attacker can compromise a vulnerable system, testers will be required to demonstrate exploits in a controlled environment without actually making the infrastructure unavailable, unless that’s a requirement.

Penetration Testing is the next step to Vulnerability Assessment aiming to penetrate the target system based on exploits available for the identified vulnerabilities. For exploitation, our own knowledge or publicly available exploits of well-known vulnerabilities can be utilized.Penetration Testing or Vulnerability Exploitation can be broadly divided into phases such as pre exploitation, exploitation, and post exploitation.Activities in the pre-exploitation phase are explained in phases 1 to 4 that is, enumerating the infrastructure and identifying the vulnerability.

Once any vulnerability is exploited to gain access to the system, the attacker should aim to further detail the network by sniffing traffic, mapping the internal network, and trying to obtain a higher privilege account to gain the maximum level of access to the system.This will enable testers to launch further attacks on the network to further increase the scope of compromised systems.

The post exploitation step will also involve clearing of tracks by conducting activities such as clearing logs and disabling antivirus. As a post-exploitation phase tester, you can demonstrate how an attacker can maintain access to the system through backdoors and rootkits.

## Stage 6 – Report generation

After completing the assessment as per the scope of work, final reporting needs to be

done covering the following key areas:

* A brief introduction about the assessment
* The scope of assessment
* The management/executive summary
* A synopsis of findings with risk severity
* Details about each finding with their impact and your recommendations to fix the vulnerability.

**3. Market Requirements Document (MRD)**

A market requirements document (MRD) is a document that communicates the customer’s wants and needs for a product or service. It is often confused with a [product requirements document](https://www.aha.io/roadmapping/guide/requirements-management/what-is-a-prd-(product-requirements-document) (PRD), but they are not the same. The PRD describes how a product should be built and helps broader cross-functional teams understand what a product should do.

|  |  |
| --- | --- |
| Executive summary | The evolving tools, tactics and procedures used by cybercriminals to breach networks means that it’s important to regularly test your organisation’s cyber security. |
| Vision | **VAPT gives** a more detailed view of the threats that your network or application is facing. It helps enterprises to protect their data and systems from malicious attacks. ... Protects your business from data loss and unauthorized access. It will help you in protecting your data from outside and insider threats. |
| Target market | In these days of widespread Internet usage, security is of prime importance. The almost universal use of mobile and Web applications makes systems vulnerable to cyber attacks. Vulnerability assessment can help identify the loopholes in a system while penetration testing is a proof-of-concept approach to actually explore and exploit a vulnerability.  Cyber attacks are increasing every day with the increased use of mobile and Web applications. Globally, statistics show that more than 70 per cent of the applications either have vulnerabilities which could potentially be exploited by a hacker, or worse, they have already been exploited. The data losses due to this are typically of two types. Either the data is confidential to the organisation or it is private to an individual. Regardless of the category, data losses result in the loss of money or reputation. |
| Personas | As the IT Scenario is changing, it is opening up new internet security challenges being faced by many organizations. Conducting business transactions over the internet (online) has always been a risk. It’s a world of unforeseen traps, with vulnerabilities and threats manifesting themselves in the least expected place, at the least expected hour. |
| Competitor analysis | * 1. McAfee Security Services.   2. Micosoft Cybersecurity Protection.   3. Catapult Systems.   4. OneNeck IT Solutions.   5. Sophos Professional Services. |
| High-level capabilities | Those with a steady scanning cadence fix security flaws 2x faster than those with ... Veracode's service allows companies to meet their compliance requirements to protect internal systems, sensitive customer data and company reputation. |
| Metrics strategy | To determine the general security level of an analyzed network, a common process needs to be realized: First, security experts identify what should be measured. Then they organize the involved variables in a manageable and meaningful way. After that, repeatable formulas should be built to illustrate the snapshot status of security and how it changes over time. For network and/or system security measurement, most existing approaches are based on risk analysis, in 4 which security risk is expressed as a function of threats, vulnerabilities, and potential impacts (or expected loss).   * 1. Calculation of Asset Value   2. Calculation of Potential Loss   3. Measurement of Security Spending   4. Attack Risk Analysis |

**4. Product Requirements Document (PRD)**

A product requirements document (PRD) defines the value and purpose of a product or feature. It is written by the [product manager](https://www.aha.io/roadmapping/guide/product-management/what-is-the-role-of-a-product-manager) to communicate what you are building, who it is for, and how it benefits the end user. It is often confused with a market requirements document (MRD), but they are different. An MRD should be created before a PRD so you can document what the customer needs and wants from your product or service before you define the requirements.

**The key components of a product requirements document-:**

**a. Objective**

The objective of VAPT Vulnerability Assessment and Penetration Testing (VAPT) is to identify all potential loopholes within your network **security** system and show the potential impact of those threats and loopholes by exploiting them.

|  |  |
| --- | --- |
| **Vision** | The scope of penetration and [security testing](https://www.kratikal.com/) in India is tremendous in today’s time. Cyber attacks becoming the norm, it is more important than ever before to undertake regular vulnerability scans and [penetration testing](https://www.kratikal.com/managed-security.php) to identify vulnerabilities and ensure on a regular basis that the cyber controls are working. |
| **Goals** | Vulnerability Assessment and Penetration Testing (VAPT) are both **security** services that focus on identifying vulnerabilities in the network, server and system infrastructure. Both the services serves a different purpose and carried to achieve different but complimentary goals. |

**b. Features**

The next step is to define each [feature](https://www.aha.io/roadmapping/guide/requirements-management/what-are-product-features) (or user story) that will be delivered in the release. This section of the PRD is where you explain exactly what needs to be built so the development team can determine how best to implement it.

Use this template to document the product requirements for each feature.

|  |  |
| --- | --- |
| **Feature** | It provide security to our websites. |
| **Description** | The **objective** of **VAPT** Vulnerability Assessment and Penetration Testing (**VAPT**) is to identify all potential loopholes within your network security system and show the potential impact of those threats and loopholes by exploiting them |
| **Purpose** | The purpose of vapt is that to make the websites secure so no one can hack the websites and our data remain safe with us. |
| **User problem** | User are facing problem as there sites get hacked and there data get lost . |
| **User value** | The solution help the user by securing there websites and not facing any of the further problems like hacking and data shared through hack. |

**c. User flow and design**



**Conlusion**

This is to conclude that the project that we undertook was worked upon with a sincere effort. Most of the requirements have been fulfilled up to the mark and the requirements which have been remaining, can be completed with a short extension. This project would definitely satisfy all the requirements of the college and would be beneficial for the students and the college staff. We find the vulnerabilities in the website of successfully with the help of above tools and it is very interesting to hack into the website and make report of it.