UNIT 4

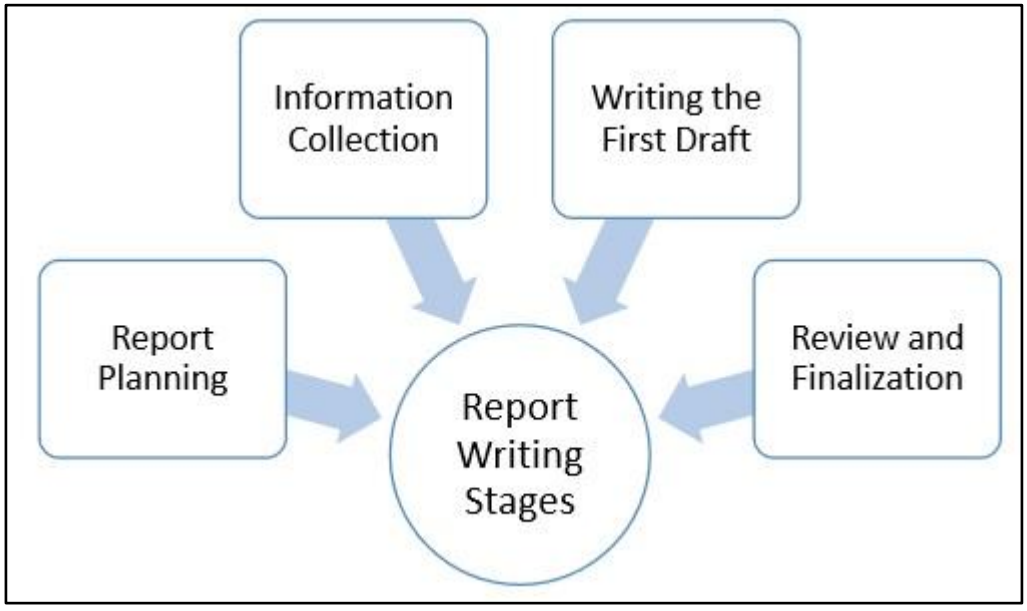
What is Report Writing?

In penetration testing, report writing is a comprehensive task that includes methodology, procedures, proper explanation of report content and design, detailed example of testing report, and tester's personal experience. Once the report is prepared, it is shared among the senior management staff and technical team of target organizations. If any such kind of need arises in future, this report is used as the reference.

Report Writing Stages

Due to the comprehensive writing work involved, penetration report writing is classified into the following stages −

- Report Planning
- Information Collection
- Writing the First Draft
- Review and Finalization



Report Planning

Report planning starts with the objectives, which help readers to understand the main points of the penetration testing. This part describes why the testing is conducted, what are the benefits of pen testing, etc. Secondly, report planning also includes the time taken for the testing.

Major elements of report writing are −

- **Objectives** − It describes the overall purpose and benefits of pen testing.
- **Time** − Inclusion of time is very important, as it gives the accurate status of the system. Suppose, if anything wrong happens later, this report will save the tester, as the report will illustrate the risks and vulnerabilities in the penetration testing scope during the specific period of time.
- **Target Audience** − Pen testing report also needs to include target audience, such as information security manager, information technology manager, chief information security officer, and technical team.
- **Report Classification** − Since, it is highly confidential which carry server IP addresses, application information, vulnerability, threats, it needs to be classified properly. However, this classification needs to be done on the basis of target organization which has an information classification policy.
- **Report Distribution** − Number of copies and report distribution should be mentioned in the scope of work. It also needs to mention that the hardcopies can be controlled by printing a limited number of

copies attached with its number and the receiver's name.

Information Collection

Because of the complicated and lengthy processes, pen tester is required to mention every step to make sure that he collected all the information in all the stages of testing. Along with the methods, he also needs to mention about the systems and tools, scanning results, vulnerability assessments, details of his findings, etc.

Writing the First Draft

Once, the tester is ready with all tools and information, now he needs to start the first draft. Primarily, he needs to write the first draft in the details – mentioning everything i.e. all activities, processes, and experiences.

Review and Finalization

Once the report is drafted, it has to be reviewed first by the drafter himself and then by his seniors or colleagues who may have assisted him. While reviewing, reviewer is expected to check every detail of the report and find any flaw that needs to be corrected.

Requirements of low level and high level Penetration Test Report?

Penetration test reports are very important and provide you with the structured detailed of the pentest after the engagement has completed. However oftentimes this critical documentation lacks key aspects of what should be included, and clients begin to question the practical value of their assessments—and rightfully so. The report is everything.

While there are many nice things you can include in a report

1 - Executive Summary for Strategic Direction

The executive summary serves as a high-level view of both risk and business impact in plain English. The purpose is to be concise and clear. It should be something that non-technical readers can review and gain insight into the security concerns highlighted in the report.

While IT staffers may need all the technical details, executives don't need to understand *the technology*. They need to understand business risk, something a good executive summary will effectively communicate. It is imperative that business leaders grasp what's at stake to make informed decisions for their companies, and the executive summary is essential to delivering that understanding.

Visual communication can also be helpful in getting complex points across clearly. Look for graphs, charts, and similar visuals in communicating the summary data provided here

2 - Walkthrough of Technical Risks

Most reports use some sort of rating system to measure risk, but seldom do they take the time to *explain* the risk. The client's IT department needs to make swift, impactful decisions on how best to resolve vulnerabilities. To do so, they require approval from the people upstairs. To simply state that something is dangerous does not properly convey risk.

For instance, if a critical vulnerability is found allowing file-uploads to a healthcare portal, there are two ways to report this:

1 – Technically Accurate – Company X's web application does not limit user uploads by file type, creating a vulnerability that allows an attacker to execute arbitrary code remotely and elevate their privilege within the application.

2 – Both Accurate and Contextualized – Company X's web application does not limit user uploads by file type, creating a vulnerability that allows an attacker to execute arbitrary code remotely and elevate their privilege within the application. In this instance, the attacker would be able to view the medical records of any user and operate as an administrator on the application.

The second one has a more weight to it, indicating not only the technical aspects but the business impact as well. The most valuable reports are

those that speak to all audience members in the language they understand – especially those in leadership positions.

For instance, if your team finds that a client's healthcare management web portal allows users to upload a profile picture, but does not prevent them from uploading arbitrary code instead, there are essentially two ways to report this:

3 - Potential Impact of Vulnerability

Risk can be broken down into two pieces: likelihood and potential impact.

Likelihood is standard in most assessment reports. Of course, the odds of an exploitation—while important—aren't enough to define risk. You wouldn't rank a deep-seated remote code execution lower than an email address of a developer obviously present in an HTML script. This is because the former would be far more impactful to the client.

If you think you're seeing a theme here, you're not wrong. An assessment report isn't *just* for the IT staff. Executives need to see a break-down of how a vulnerability that anyone could have would directly affect their organization specifically. Factoring both the likelihood and potential impact of an exploitation into the overall risk is a major component in an excellent report.

4 - Multiple Vulnerability Remediation Options

Most penetration test reports will include a generic, high-level description of how to handle these problems; however, these generic "catch-all' remediation guides often fall short when it comes to the unique context of the client's needs. If a client has a vulnerable service running on a webserver that they depend on, the remediation should offer more than telling them to simply disable the service altogether.

Of course, it's important to let the client know that there's a straightforward method of filtering for SQL injections, or configuring their firewall to block certain attacks. That said, a quality pentest report will give you multiple remediation options that are detailed enough to prepare the client's IT team for a swift resolution. Assuming the internal staff already knows how to remediate all vulnerabilities greatly reduces the value of the penetration test.

VULNERABILITIES AND MITIGATION ISSUES

VULNERABILITY MANAGEMENT DEFINED

Vulnerabilities are weaknesses or other conditions in an organization that a threat actor, such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to adversely affect data security. Cyber vulnerabilities typically include a subset of those weaknesses and focus on issues in the IT software, hardware, and systems an organization uses. For example:

Design, implementation, or other vendor oversights that create defects in commercial IT products . Poor setup, mismanagement, or other issues in the way an organization installs and maintains its IT hardware and software components.

Vulnerability management programs address these issues. Other common vulnerabilities that organizations must also tackle in their information security programs include:

- Gaps in business processes.
- Human weaknesses, such as lack of user training and awareness.
- Poorly designed access controls or other safeguards.
- Physical and environmental issues.

Vulnerability management programs:

Define a formal process to:

- timely identify applicable vulnerabilities
- close the security gaps that vulnerabilities create by remediating or at least mitigating their effects;
- track and document an organization’s efforts.

Prioritize often limited IT resources. Organizations must focus on vulnerabilities according to their level of risk, particularly considering the sheer volume of changes that diligent vulnerability management can demand.

Continuously monitor and evaluate an organization's IT environment to ensure compliance and avoid re-introduction of known vulnerabilities

Minimize cyber attack risks by decreasing the number of gaps that attackers can exploit, also known as the organization's "attack surface."

MITIGATING AND REMEDIATING IDENTIFIED VULNERABILITIES

Organizations typically remediate identified vulnerabilities by:

Applying patches or other vendor-supplied updates for hardware and software defects

Updating configurations to use more secure settings or deactivate unnecessary services or communication channels.

Some organizations use automated software distribution tools or other products to apply patches and track software updates, especially those with large or complex IT environments. Smaller organizations with simple environments that consistent mainly of end user devices may depend on vendors' automatic update features, such as Microsoft's Windows Update.

Some systems cannot tolerate patching because:

- Testing for internally or custom-developed software fails.
- Different vendor product combinations create incompatibilities.

Organizations may require additional time to patch systems that run highly available business critical operations. Patches may not be available for older legacy systems that organizations still depend on for important business functions.

Mitigation techniques or compensating controls help manage risks on these systems. For example, an organization may isolate vulnerable systems on dedicated network segments or apply additional access, auditing, or monitoring controls.

Organizations with more complex environments, especially those with internally or custom-developed software, generally test patches and other

remediation measures in dedicated testing environments before deployment. Software patches can have unintended effects, so remediation plans should include system restoral options. Organizations should integrate their vulnerability mitigation and remediation activities into existing IT change management procedures to avoid inadvertent business impact.

Mitigation and remediation activities are not complete until they update the organization’s asset inventory to document changes made and software installed