
Chapter 12. Documentation and Reporting

Assessment tracking and documentation is a critical aspect of professional penetration testing. Each input and output from the testing tools should be recorded to ensure that the findings are reproducible in an accurate and consistent manner when needed. Keep in mind that part of the penetration testing process includes presenting the findings to clients. There is a high likelihood that these clients will want to mitigate the vulnerabilities and then attempt to mimic your steps in order to ensure their mitigations were effective. Depending on the scope, you may be required to perform additional testing that verifies any improvements the client makes, which actually removes the vulnerabilities you found. Accurate documentation of your steps will assist you in ensuring that the very same testing occurs during this follow up.

Proper test documentation provides a record of the actions performed and thus allows you to trace your steps in case the business experiences non-test related incidents during your agreed upon test window. A detailed recording of your actions can be very tedious, but as a professional penetration tester, this step should not be overlooked.

Documentation, report preparation, and presentation are the core areas that must be addressed in a systematic, structured, and consistent manner. This chapter provides detailed instructions that will assist you in aligning your documentation and reporting strategy. The following topics will be covered in this chapter:

- Results verification ensures that only validated findings are reported.
- Types of reports and their reporting structures will be discussed in the paradigm of an executive, management, and technical perspective to reflect the best interests of the relevant authorities involved in the penetration testing project.
- The presentation section provides general tips and guidelines that may help in understanding your audience and their level of tactfulness to the given information.
- Post-testing procedures, the corrective measures, and recommendations that you should include as a part of a report, and use them for advising the remediation team at the concerning organization. This kind of exercise is quite challenging and requires an in-depth knowledge of a target infrastructure under security considerations.

Each of the following sections will provide a strong basis for preparing documentation, reporting, and presentation, and especially highlighting their roles. Even a small mistake can lead to a legal problem. The report that you create must show consistency with your findings, and should do more than just point out the potential weaknesses found in a target environment. For instance, it should be well prepared and demonstrate a proof of support against known compliance requirements, if any, required by your client. Additionally, it should clearly state the attacker's modus operandi, applied tools and techniques, and list the discovered vulnerabilities and verified exploitation methods. Primarily, it is about focusing on the weaknesses rather than explaining a fact or procedure used to discover them.

Documentation and results verification

A substantial amount of vulnerability verification will be necessary in most cases to ensure that your findings are actually exploitable. Mitigation efforts can be expensive and as such, vulnerability verification is a critical task in terms of your reputation and integrity. In our experience, we have noticed several situations where people just run a tool, grab the results, and present them directly to their clients. This type of irresponsibility and lack of control over your assessment may result in serious consequences and cause the downfall of your career. In situations where there are false negatives, it might even place the client at risk by selling a false sense of security. Thus, the integrity of test data should not be tainted with errors and inconsistencies. Following are a couple of procedures that may help you in documenting and verifying the test results before being transformed into a final report:

- Take detailed notes of each step that you have taken during the information gathering, discovery, enumeration, vulnerability mapping, social engineering, exploitation, privilege escalation, and persistent access phases of the penetration testing process.
- Make a note-taking template for every single tool you executed against your target from Kali. The template should clearly state its purpose, execution options, and profiles aligned for the target assessment, and provide space for recording the respective test results. It is also essential to repeat the exercise (at least twice) before drawing the final conclusion from a particular tool. In this way, you certify and test-proof your results against any unforeseen conditions. For instance, while using Nmap for the purpose of port scanning, we should layout our template with necessary sections, such as usage purpose, target host, execution options, and profiles (service detection, OS type, MAC address, open ports, device type, and so on), and document the output results accordingly.
- Do not rely on a single tool. Relying on a single tool (for example, for information gathering) is absolutely impractical, and may introduce discrepancies to your penetration testing engagement. Thus, we highly encourage you to practice the same exercise with different tools made for a similar purpose. This will ensure the verification process' transparency, increase productivity, and reduce false positives and false negatives. In other words, every tool has its own specialty to handle a particular situation. It is also counted to test certain conditions manually wherever applicable, and use your knowledge and experience to verify all the reported findings.

Types of reports

After gathering every single piece of your verified test results, they must be combined into a systematic and structured report before submitting to the target stakeholder. There are three different types of reports; each has its own schema and layout relevant to the interests of a business entity involved in the penetration testing project. The types of reports are as follows:

- Executive report
- Management report
- Technical report

These reports are prepared according to the level of understanding and ability to grasp the information conveyed by the penetration tester. We have detailed each report type and its reporting structure with basic elements that may be necessary to accomplish your goal. It is important to note that all of these reports should abide by non-disclosure policy, legal notice, and penetration testing agreement before being handed to the stakeholders.

The executive report

The executive report, a type of assessment report, is shorter and more concise to point the high-level view of the penetration testing output from a business strategy perspective. The report is prepared for C level executives within a target organization (CEO, CTO, CIO, and so on). It must be populated with some basic elements as follows:

- **Project objective**: This section defines the mutually agreed criteria for the penetration testing project between you and your client.
- **Vulnerability risk classification**: This section explains the risk levels (critical, high, medium, low, and informational) used in the report. These levels should clearly differentiate and highlight the technical security exposure in terms of severity.
- **Executive summary**: This section briefly describes the purpose and goal of the penetration testing assignment under the defined methodology. It also highlights the number of vulnerabilities discovered and exploited successfully.
- **Statistics**: This section details the vulnerabilities discovered in the target network infrastructure. These can also be drawn in the form of a pie chart or in any other intuitive format.
- **Risk matrix**: This section quantifies and categorizes all the discovered vulnerabilities, identifies the resources potentially affected, and lists the discoveries, references, and recommendations in a shorthand format.

It is always an idealistic approach to be creative and expressive while preparing an executive report and to keep in mind that you are not required to reflect upon the technical grounds of your assessment results, but rather give factual information processed from those results. The overall size of the report should be two to four pages.

The management report

The management report is generally designed to cover the issues including regulatory and compliance measurement in terms of target security posture. Practically, it should extend the executive report with a number of sections that may interest the **Human Resource** (**HR**) and other management people, and assist in their legal proceedings. Following are the key parts that may provide you with valuable grounds for the creation of such a report:

- **Compliance achievement**: This initiates a list of known standards and maps each of its sections or subsections with the current security disposition. It should highlight any regulatory violations that occurred, which might inadvertently expose the target infrastructure and pose serious threats.
- **Testing methodology**: This should be described briefly and should contain enough details that may help the management people to understand the penetration testing lifecycle.
- **Assumptions and limitations**: This highlights the known factors that may have prevented the penetration tester from reaching a particular objective.
- **Change management**: This is sometimes considered a part of the remediation process; however, it is mainly targeted towards the strategic methods and procedures that handle all the changes in a controlled IT environment. The suggestions and recommendations that evolve from security assessment should remain consistent with a change in the procedures, in order to minimize the impact of an unexpected event upon the service.
- **Configuration management**: This focuses on the consistency of the functional operation and performance of a system. In the context of system security, it follows any change that may have been introduced to the target environment (hardware, software, physical attributes, and others). These configuration changes should be monitored and controlled to maintain the system configuration state.

As a responsible and knowledgeable penetration tester, it is your duty to clarify any management terms before you proceed with the penetration testing lifecycle. This exercise definitely involves one-to-one conversations and agreements on target-specific assessment criteria, such as what kind of compliance or standard frameworks have to be evaluated, are there any restrictions while following a particular test path, will the changes suggested be sustainable in a target environment, or will the current system state be affected if any configuration changes are introduced. These factors all jointly establish a management view of the current security state in a target environment, and provide suggestions and recommendations following the technical security assessment.

The technical report

The technical assessment report plays a very important role in addressing the security issues raised during the penetration testing engagement. This type of report is generally developed for techies who want to understand the core security features handled by the target system. The report will detail the vulnerabilities, how they can be exploited, what business impact they could bring, and how resistant solutions can be developed to thwart any known threats. It has to communicate with all-in-one secure guidelines for protecting the network infrastructure. So far, we have already discussed the basic elements of the executive and management reports. In the technical report, we extend these elements and include some special themes that may draw substantial interests for the technical team at the target organization. Sometimes, sections such as project objectives, vulnerability risk classification, risk matrix, statistics, testing methodology, and assumptions and limitations are also a part of the technical report. The technical report consists of the following sections:

- **Security issues**: The security issues raised during the penetration testing process should be clearly cited in detail, such that for each applied attack method, you must mention the list of affected resources, its implications, original request and response data, simulated attack request and response data, provide reference to external sources for the remediation team, and give professional recommendations to fix the discovered vulnerabilities in the target IT environment.
- **Vulnerabilities map**: This provides a list of discovered vulnerabilities found in the target infrastructure, each of which should be easily matched to the resource identifier (for example, the IP address and target name).
- **Exploits map**: This provides a list of the successfully checked and verified exploits that worked against the target. It is also crucial to mention whether the exploit was private or public. It may be beneficial to detail the source of the exploit code and for how long it has been available.
- **Best practices**: This emphasizes the better design, implementation, and operational security procedures the target may lack. For instance, in a large enterprise environment, deploying an edge-level security could be advantageous to reduce the number of threats before they make their way into a corporate network. Such solutions are very handy and do not require technical engagement with production systems or legacy code.

Generally speaking, the technical report brings forward the ground realities to the associative members of the organization concerned. This report plays a significant role in the risk management process and will likely be used to create actionable remediation tasks.

Network penetration testing report (sample contents)

Just as there are different types of penetration testing, there are different types of report structures. We have presented a generic version of a network-based penetration testing report that can be extended to utilize almost any other type (for example, web application, firewall, wireless networks, and so on). In addition to the following table of contents, you would also want a cover page which states the testing company's name, type of report, scan date, author name, document revision number, and a short copyright and confidential statement.

The following would be the table of contents for a network-based penetration testing report:

- Legal notice
- Penetration testing agreement
- Introduction
- Project objective
- Assumptions and imitations
- Vulnerability risk scale
- Executive summary
- Risk matrix
- Testing methodology
- Security threats
- Recommendations
- Vulnerabilities map
- Exploits map
- Compliance assessment
- Change management
- Best practices
- Annexes

As you can see, we have combined all types of reports into one single complete report with a definitive structure. Each of these sections can have its own relevant subsections that can better categorize the test results in a greater detail. For instance, the annexes section can be used to list the technical details and analysis of a test process, logs of activities, raw data from various security tools, details of the research conducted, references to the Internet sources, and glossary. Depending on the type of report being requested by your client, it is solely your duty to understand the importance and value of your position before beginning a penetration test.

Preparing your presentation

It is helpful to understand the technical capabilities and goals of your audience in order to accomplish a successful presentation. You will need to tweak the material according to your audience; otherwise, you will face a negative reaction. Your key task is to make your client understand the potential risk factors surrounding the areas you have tested. For instance, managers at executive level may not have time to worry with the details of a social engineering attack vector, but they will be interested in knowing the current state of security and what remediation measures should be taken to improve their security posture.

Although there is no formal procedure to create and present your findings, you should keep a professional outlook to make the best of your technical and non-technical audiences. It is also a part of your duty to understand the target environment and its group of techies by gauging their skill levels and helping them know you well, as much as any key asset to the organization.

Pointing out the deficiencies in the current security posture and exposing the weaknesses without emotional attachment can lead to a successful and professional presentation. Remember, you are there to stick with your facts and findings, prove them technically, and advise the remediation team accordingly. As this is a kind of face-to-face exercise, it is highly advisable to prepare yourself in advance to answer the questions supporting the facts and figures.

Post-testing procedures

Remediation measures, corrective steps, and recommendations are all terms referring to the post testing procedures. During this procedure, you act as an advisor to the remediation team at the target organization. In this capacity, you may be required to interact with a number of technical people with different backgrounds, so keep in mind that your social appearance and networking skills can be of great value here.

Additionally, it is not possible to hold all sets of knowledge required by the target IT environment unless you are trained for it. In such situations, it is quite challenging to handle and remediate every single piece of vulnerable resource without getting any support from the network of experts. We have constituted several generic guidelines that may help you in pushing critical recommendations to your client:

- Revisit the network design and check for exploitable conditions at vulnerable resources pointed in the report.
- Concentrate on the edge-level or data centric protection schemes to reduce the number of security threats before they strike with backend servers or workstations simultaneously.
- Client-side or social engineering attacks are nearly impossible to resist but can be reduced by training the staff members with the latest countermeasures and awareness.
- Mitigate system security issues as per the recommendations provided by the penetration tester may require additional investigation to ensure that any change in a system should not affect its functional characteristics.
- Deploy verified and trusted third-party solutions (IDS/IPS, firewalls, content protection systems, antivirus, IAM technology, and so on) where necessary, and tune the engine to work securely and efficiently.
- Use the divide-and-conquer approach to separate the secure network zones from insecure or public-facing entities on the target infrastructure.
- Strengthen the skills of developers in coding secure applications that are a part of the target IT environment. Assessing application security and performing code audits can bring valuable returns to the organization.
- Employ physical security countermeasures. Apply a multilayered entrance strategy with a secure environmental design, mechanical and electronic access control, intrusion alarms, CCTV monitoring, and personnel identification.
- Update all the necessary security systems regularly to ensure their confidentiality, integrity, and availability.
- Check and verify all the documented solutions provided as a recommendation to eliminate the possibility of intrusion or exploitation.

Summary

In this chapter, we have explored some basic steps necessary to create a penetration testing report and discussed the core aspects of doing a presentation in front of the client. At first, we fully explained the methods of documenting your results from individual tools and suggested not to rely on single tools for your final results. As such, your experience and knowledge counts in verifying the test results before being documented. Make sure to keep your skills updated and sufficient to manually verify the findings when needed. Afterwards, we shed light on creating different types of reports with their documentation structures. These reports mainly focus on executive, managerial, and technical aspects of a security audit we carried out for our client. Additionally, we also provided a sample table of contents for a network-based penetration testing report to give you a basic idea for writing your own report. Thereafter, we discussed the value of live presentation and simulations to prove your findings, and how you should understand and convince your audiences from different backgrounds.

Finally, we have provided a generic list of the post testing procedures that can be a part of your remediation measures or recommendations to your client. This section provides a clear view of how you assist the target organization in the remediation process, being an advisor to their technical team or remediate yourself.