
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.