Composing a Penetration Report

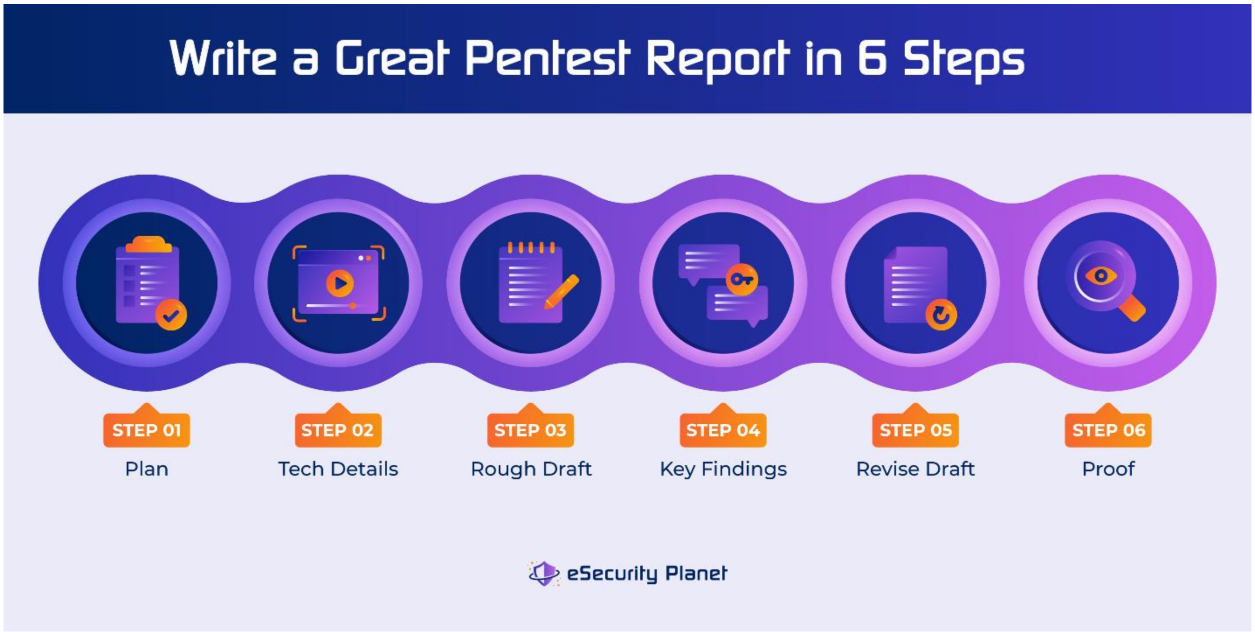
A penetration testing report discloses the vulnerabilities discovered during a penetration test to the client.

A pentest report should also outline the vulnerability scans and simulated cybersecurity attacks the pentester used to probe for weaknesses in an organization’s overall security stack or specific systems, such as websites, applications, networks, and cloud infrastructure.

To be truly useful, the report must be more than a simple list. Penetration test reports deliver the only tangible evidence of the pentest process and must deliver value for a broad range of readers and purposes.

How to Write a Great Pentest Report in 6 Steps

The process of writing a great penetration test report is straightforward and can be covered in six key steps. Each step builds on the previous step to increase the quality of the information, the organization of the findings, and the usability of the report for stakeholders.



1. **Plan:** Outlining the testing and creating report templates in advance acts both as a checklist of information needed and as a repository for testing details.
2. **Capture the technical details:** Include notes, screenshots, and log files in the report, but to make documentation less disruptive, take video and narrate while conducting the pentest and take screenshots later.
3. **Start with a rough draft:** Begin with the most significant vulnerabilities, remediations, and overall results. Don't worry about grammar, spelling, or complete sentences just yet.
4. **Categorize and summarize key findings:** Including criticality, vulnerability, system, and other important findings will help clients address issues by the level of risk they pose.
5. **Revise the draft:** Here's where you focus on grammar, punctuation, and spelling to turn the content into plain, formal English, using non-technical language to help IT generalists and managers understand the risks.
6. **Organize and proofread:** Double check the information to eliminate errors, make the report easy to read, and to focus on the most important findings; move non-critical information to appendices.

Although the process is simple enough, a quality report relies on the proper execution of this process and the inclusion of expected information.

There are many ways to write a penetration testing report. Fortunately, most tests will share several key sections such as an **executive summary, recommendations and remediations, findings and technical details, and finally, the appendices**. These sections are the foundations of your report.

Executive Summary

Objective: Clearly explain the risks that discovered vulnerabilities present and how they'll affect the future of the organization if exploited.

Length: One or two pages. Anything more is not a summary, and will probably be overlooked. Being precise and concise is paramount

Any report worth reading should include an executive summary to help non-technical leaders digest and determine strategic action based on the information in your report. This section is arguably one of the most important since it will provide leadership with a bottom line up front (BLUF) summary of what was done, where defenses excelled, and what failed to stop you, the attacker.

Keep in mind that your target audience during this part of the report are decision-makers who allocate funds to forward remediations (not technical staff who execute changes). For this reason, we want to ensure that it is easily understood and should therefore avoid using acronyms, infosec jargon, and including overly technical details.

Providing helpful recommendations such as changes to processes, hardening of application and hardware settings, and even educational solutions is a great way to finish writing the executive summary. Although, it isn't a sales pitch. So ensure that any recommendations provided are vendor agnostic.

Recommendations or remediations

Objective: Provide the client with recommendations for short, medium, and long-term implementation that will improve their security posture.

Length: Ideally, you want to report everything to the customers, but this could become cumbersome depending on the severity of your findings. Including the findings that are of critical, high, and maybe even medium importance is a must. If you have a large number of findings, especially in the low and informational importance, it may be best to include them all in an appendix attached to the report instead of writing a 400-page report filled with extra information

This section provides the customer with a set of recommendations for their short, medium, and long-term implementation. To ensure that recommendations are effective and that risks are represented accurately, use a scoring system and classification set like the Common Vulnerability Scoring System (CVSS) or Common Vulnerabilities and Exposures (CVEs).

Just like a doctor's assessment and diagnosis of a serious medical condition, a second opinion is always useful for ensuring a high degree of accurate and effective remediations. With that in mind, relevant third-party links and resources that discuss highlighted issues are also useful to include. .

Technical Findings

Objective: Deliver technical details of how clients can remediate the security flaws that you found.

Length: Length doesn't matter here, but want to be clear and concise in demonstrating the path you took and the actions required. Defenders should be able to replicate the attack based solely on your documentation of it. Screenshots are perfect for this purpose.

This section is written for those who will be implementing fixes based on our findings. We want to be as descriptive and specific as possible. This means providing the following information:

Your methodology

Write this as you go (which again reinforces the importance of taking notes). It should show your full stream of thought and actions as you progressed through the assessment.

Objectives

What was your mission?

If the objective was to acquire domain administrative access or to display the ability to exfiltrate data from the customer's network, be sure to communicate that. Clearly communicating your mission is key because the technicians who read your report may not have been aware of the assessment.

Scope

Document the agreed scope to include any hosts, IP address blocks, specific domains, and/or any specific applications or hardware that was to be tested. You want to ensure that technical teams understand what resources were excluded from testing since they could be potential blind spots for them.

Details

This is where we document how we completed our tasks or how we were rebuffed by the customer’s defenses.

Attack Chains

Share your successful chains along with those that failed. This lets organizations know where their defenses are working, and what needs attention. These assessments are meant to provide actionable information for the customer, not a highlight reel of our skills.

We can show our methodology in detail here with the use of shell output, screenshots, and supporting documentation such as scan outputs, write-ups of Proofs of Concept, and more. Most importantly, this information should make our actions repeatable so that teams can validate and secure the issues at hand.

Appendices

Objective: Deliver technical details of how clients can remediate the security flaws that you found.

Length: The more you can provide to prove your case, the better your report will be.

The appendices will hold any supporting output, screenshots, and documentation needed to provide proof of your actions and to demonstrate the potential impact your attack path had.

These can be in the form of attachments or directly included in the report. These appendices could include Bloodhound output, lists of credentials discovered and cracked, user data, NMAP scans, and anything else of note.

How to make your penetration testing reports stand out

1. Know your audience: Tailor the different sections to the audience. For example, the executive summary is probably the only thing that executives are going to read. Keep it high level and focus on the things that impact the business and actually pose significant risks to critical systems/clients/data.

2. Take extensive notes: Include any tools or tactics that you've tried, especially those that failed. Sometimes you'll want to revisit systems after learning something new and realize that a tactic you tried previously would have worked if you had that information when you tried the first time around.

3. Simplify complex topics: Our roles as penetration testers can be highly technical and extremely complex. Nevertheless, if we can't explain something complex in a concise, easy-to-understand manner, we'll limit our ability to help customers and provide value to our employers.

4. Collaborate when possible: Many of us will find ourselves working with a team of testers to ensure quality work. Setting up a shared space for report writing, collection of artifacts and general collaboration will ensure that everyone is on the same page. This will improve your report and the feedback you provide to your customers.

5. Proofread to protect credibility: The credibility of an otherwise strong penetration testing report can be derailed by simple errors like spelling and grammar mistakes. Use some form of grammar checking, (Grammarly is my favorite), and ideally, have another team member read it over from a different perspective.

Our end goal as penetration testers should always be to craft a story that attempts to answer all of the following important questions:

How did you find the issue?

What is the root cause or vulnerability?

How hard was it to take advantage of the vulnerability?

Is it possible to use this vulnerability for further access?

Potential impact on the organization? (loss of resources, loss of funds, damage to equipment, theft of IP)

How can it be fixed or mitigated?