Pentesting 101 Part 4: Penetration Test Report & Debrief - The Deliverables

labs.lares.com/pentesting-101-pt4

Steve Spence March 13, 2024

penetrationtesting

This part of the series will focus on what a penetration testing report should contain and how we use the penetration engagement, the testing activities carried out, and the information, vulnerability, and/or exploit data we documented to populate the penetration testing report.

Steve Spence

Mar 13, 2024 • 9 min read

Hacking is the fun part; now, for the business end of things, it is the most crucial output.

Following our previous posts, Part1, Part 2, Part3, let's continue building on what we have learned, identified, carried out, and moved towards our end goal.

So, a quick recap … again!

- We’ve identified the reason for driving/your need to conduct a penetration test, as well as any required testing types.
- We’ve identified our engagement prerequisites and the scope of the penetration testing.
- We've carried out our penetration testing activities as defined by our agreed Scope of Work.
- We have documented any observations, findings, evidence and exploitation.

Where Do We Start?

We are at the stage where we have everything we need to compile our report. From an engagement and business point of view, this is ultimately the deliverable.

A good friend and colleague of mine regularly says:

> We get paid to write reports, the hacking is free.

This is definitely true!

In Part 3 of our series, I briefly discussed reporting and the debrief and explained that the main deliverable of any penetration test is a formal penetration/engagement test report.

The test team will write an engagement overview and assemble the findings with associated risk ratings to compile a report. The resulting report is then peer-reviewed by Senior or Principal consultants. Once ready, the final report will be sent directly to the customer and/or related in-house security/technical teams (where agreed upon *in advance).*

Ultimately, the analysis and reporting of the engagement should include:

- Any security issues uncovered.
- The test team's assessment of the level of risk of each finding.
- A method of resolving each issue found.
- An opinion on the risk of your organization's security posture based on the evidence from the penetration testing carried out.

Note: It is important to remember that penetration testing should not be used to drive your organization's vulnerability management process; it is entirely the reverse. Your organization's vulnerability management process must be the driving factor when conducting penetration testing activities and assessments.

A typical penetration testing engagement report, at a minimum, should have the following sections:

- Executive Summary
- Technical Summary
- Engagement Overview
- Engagement Phases and Detailed Findings
- Supplemental Data
- Appendices

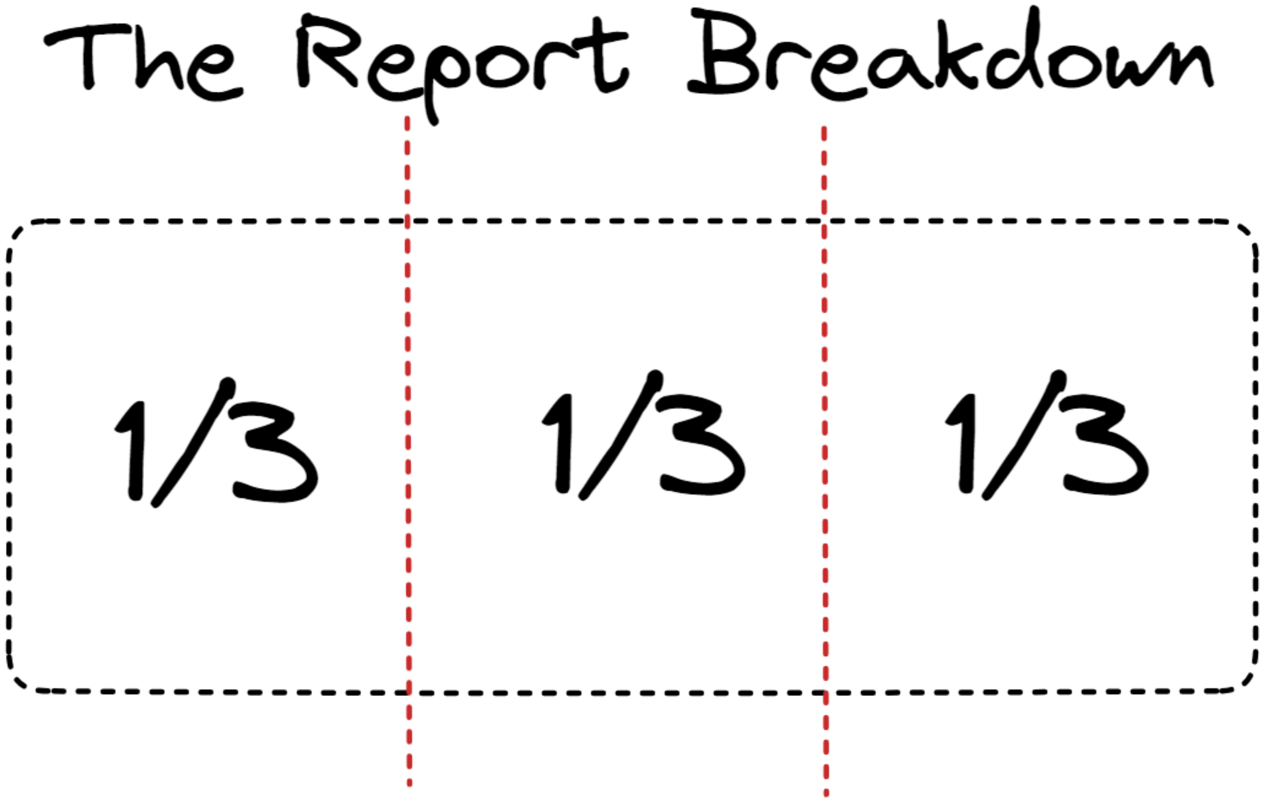
That said, when it comes to writing the penetration testing report itself, it will most likely NOT happen in the order listed above. Most, if not all, penetration testers will write their report in reverse:

- Detailed Findings

  includes annotating/marking items for inclusion within a standalone appendices section, if required

- Technical Summary
- Engagement Overview
- Executive & Assessment Summaries
- Appendices

Key Point to Remember... Target Audience



Report Breakdown

Three distinct types of readers will generally read a report; as such, the report itself needs to be written in a manner that is digestible by each group:

- **C-Level:** They usually have minimal time on their hands and, as a result, will probably not have the time to read beyond the first few pages (if that). For this reason, a visual representation of findings to indicate the areas where they need to invest, immediate risks to the business, and any impact on the business's operations is a good idea.
- **Security/Project Managers & Stakeholders:** These sections are generally read from the start of the report to the business and technical summaries, along with the engagement findings overview. Therefore, these sections need to detail the issues and their associated impacts in an understandable and actionable manner. They will need technical details and remediation advice. Details of the overall trends observed during the engagement will enable them to present results to the risk committee and executive board.

- **Technical folks:** e.g., Security, IT, Network and App teams, DevOps, Developers, etc. These folks will read the vulnerabilities and findings they have been told to fix. The findings section will need clear details on reproducing the identified issue, a recommendation, and references to enable them to deploy a fix.

The Report ...

Let us get down to Reporting.

So now we know the typical sections a penetration testing engagement report should have. Let's expand on each section, digging deeper into its purpose and how and why each is useful in communicating any risk, impact, and overall outcome of the engagement.

First up, we have:

Executive Summary Section

How different testing companies approach this section can be a mixed bag. Ideally, it should be inclusive of the following or incorporate the following:

- Executive Overview
  e.g., It should contain the client name, testing company name, dates when the work took place and type of assessment.
- Assessment Summary
  e.g., Still high-level at this stage, though should contain more about what type of testing took place, testing actions and a general indiaction of the overall risk and testing outcome.
- Engagement Recommendations
  e.g., Still high-level, these should be overall and accumulative, recommendations and not specific *(at this stage)*, unless there is an overall need to. These recommendations normally centre around reviewing current policy & procedures around risk prevention, mitigation and vulnerability patching etc

In short, this section will provide and/or describe a high-level overview of the engagement's purpose, objectives, general scope, and limitations.

Next Up, we have the following:

Technical Details Summary Section

This section will provide and/or describe a more specific, detailed, and technical account of the engagement, along with the associated phases and work undertaken by the test team.

Key points to look out for are:

- Assessment Contact Information
- Scope of Work (SoW)
- Scope & Engagement Caveats or Limitations
- Post Engagement Clean Up
- Risk Ratings Explanation *(pre-agreed risk ratings)*

Note: Information in several sections listed above can and should be populated from the engagement scoping questionnaire, scoping calls/meetings and data returned from the engagement itself.

This should then naturally be followed by a more concise section:

Engagement Overview Section

The engagement overview section should consist of the technical findings per phase. This is generally in the form of a table *(or similar)* for each phase, which will be used to communicate details, such as:

- Risk Rating
- Affected component/host
- Finding(s) discovered

Note: *This is again used to provide a high-level overview of issues discovered; however, it is aimed more at those responsible for remediating the issues discovered; therefore, more concise and technical language would be expected here.*

Lastly, the engagement overview section should ideally serve as a segue into the "meat and potatoes" section of the report, the:

Engagement Phases and Detailed Findings Section

Whilst the report serves as the overall account of when, what, and how things were done, the detailed findings section is probably the most crucial section of a penetration testing report.

This section provides a detailed overview of the testing phases conducted and the consequent security issues and findings discovered. The main focus is that this section will be specifically for those responsible for remedying the issues found during the engagement.

Several key areas should be included. These are as follows:

- Issue Title & Risk Rating

  In keeping with the actual issue and identified risk
- Description & Evidence
  - What: Summary of issue identified
  - How: e.g., screenshots, tool and or exploitation output. Evidence such as screenshots and tool/exploit output must be clear and readable
  - Steps to recreate
- Affected Components

  e.g., IP address and/or hostname
- Recommendation

  Suitable/appropriate & evidence based
- References
  - Appropriate - not a random/obscure 'blog' or 'stackoverflow' post
  - We often link to Lares Labs' blog posts when referencing previously discussed work that goes into further depth.

A note on the ‘Description’ of the issue identified. This should explain how it impacts the affected host/application/area, then detail how this risks the business, end users or interactions with both.

When reading/reviewing a penetration testing report, a handy technique to ensure that the findings the report details are fit for purpose is to identify that each finding follows along these three simple steps:

- Introduce ...

  This is where the issue/finding is described
- Show ...

  This is where what was found is documented e.g., evidence, images & steps to reproduce
- Discuss ...

  discuss the impact and risk

Note: More evidence is always better than less! Providing steps that are understandable and repeatable is vital.

Appendices

This section should be used for any information such as:

- Additional information that is provided or pertains to documented finding outlined within the ‘Engagement Phases and Detailed Findings. For example, exploitation code, proof-of-concepts etc.
- Data which would complicate any particular finding, e.g., information that degrade the overall flow and/or readability of the report.
- Glossaries
- Detailed methodologies

Tying Everything Together …

Once you've written your report, it should cover all the key areas and necessary points. It should also be digestible by the three distinct groups we outlined earlier. Lastly, it should include any potential appendices detailing more information on the findings themselves or additional supporting context to the engagement, including detailed methodologies.

The report should then be submitted for a technical peer review and quality assurance round to identify any technical inaccuracies and grammatical errors. This will ensure the report is ready for delivery and receipt by the client so that the final product is error-free and both reads and flows well.

The Debrief ...

Client Debrief

A client debrief should be offered and arranged, allowing enough time for the client and their in-house technical teams to review, digest, and understand the report, its contents, and overall risk/impact. This will also allow them to formulate appropriate follow-up questions and/or queries.

Sessions such as these can be highly beneficial for several reasons, several of which are listed below:

1. **Clear Communication of Findings:** During the debriefing session, the test team can systematically walk through their findings, detailing the vulnerabilities discovered, the methods used to exploit them, and the potential impact on the client's systems. This clear communication ensures that technical and non-technical stakeholders understand the risks identified during the assessment.
2. **Immediate Feedback and Clarification:** The client can ask questions, seek clarification, or request additional information about any specific issues identified during the penetration testing. This real-time feedback loop allows for a deeper understanding of the vulnerabilities and their potential implications, enabling the client to make informed decisions about remediation priorities and strategies.
3. **Enhanced Collaboration:** Debrief sessions foster collaboration between the test team and the client, creating an environment conducive to open dialogue and knowledge sharing. Clients may provide insights into their systems or business processes that could further contextualize the findings, while the test team can offer guidance on best practices for addressing security weaknesses.

4. **Tailored Recommendations:** During the debriefing session, the test team can discuss tailored recommendations and mitigation strategies that align with the client's needs and constraints. This personalized approach ensures that the remediation efforts are practical, effective, and feasible within the client's organizational context.
5. **Opportunity for Improvement:** Debriefing sessions allow clients to reflect on their existing security practices and processes. Organizations can refine their security policies, procedures, and training programs to better defend against future attacks by understanding how vulnerabilities were identified and exploited.
6. **Documentation and Reporting:** The debrief session serves as a forum for documenting the findings, discussions, and action items arising from the penetration testing. This formal record ensures that all stakeholders understand the assessment outcomes clearly and facilitates accountability for promptly addressing security issues.

Let’s recap...

In summary, in this part of the series, we’ve discussed/walked through the following:

- A general recap and overview of a penetration testing report
- The target audience
- The sections of a penetration testing report
- A more detailed view of what each section and what to expect
- The engagement debrief and the benefits

At this stage of the series, whether you're writing or receiving a report—be it your first or 5,000th report—it is essential to ensure that what we have covered during each post directly translates to your specific needs and/or deliverables.

If you are on the receiving end of the report, hopefully, by now, you should know what to expect from the overall penetration test process. This includes identifying your testing needs, scoping the test, understanding the execution, and ultimately understanding and interpreting the report. Digesting each segment of the report should be pretty straightforward and sufficiently segment the sections between relevant teams in your organization.

Suppose you are a penetration tester just starting. In that case, hopefully, the topics and areas we have covered will empower you and instil confidence in your ability to carry out a penetration test to a benchmark standard. Ultimately, you will provide your client with a tangible, structured engagement process, execution of work, and penetration testing report at the end of everything.

If you are ever in doubt or unsure about your penetration testing needs, seeking assistance from a dedicated organization that provides such services regularly is the first step to maturing your security posture.

Over time, you will become more informed and able to take more ownership of this process.

How can we help?

Here at Lares, we help empower organizations to maximize their security Potential.

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching.

If you would like any further information, you can get in touch here or head over to the Lares.com website for more information about how we can help.