How To Write A Security Assessment Report

Michael Markevich,
Cybersecurity Trainer

BSides Ljubljana 0x7E8 | 27 September 2024

About Me

- Penetration tester, IT auditor, security manager, university lecturer, etc. (in the past)
- Fractional CISO, consultant, and trainer (now)
- Based out of Oslo, Norway
- Have written many reports (and read even more)

Why Are You Here Today?

As penetration testers or IT auditors, we want to deliver our work in the most impressive and convincing manner.

Agenda

1. What makes a poor report?
2. Typical issues and mistakes
3. Essential components of a good report
4. Tools and automation
5. Practical exercise
6. Q&A and feedback

What Makes A Poor Report?

Common Issues

- Unclear target audience
- Lack of terms and definitions
- Technical weaknesses and mistakes
- Inconsistent design, layout, typos

And Even More Issues

- Lack of understanding of the business impact
- Lack of engagement with the audience

Writing A Good Report

Understand The Audience

Who will be reading your report?

Define The Structure

Typically, we include:

- Summary
- Methodology and terms/definitions
- Scope
- Findings

But what is the right sequence? Anything else to add?

Tell A Story

Everyone loves stories. So why not to tell them?

Example: a CUPS vulnerability (disclosed yesterday)

Select The Language

RFC 2119 ("Key words for use in RFCs to Indicate Requirement Levels") provides a great example of standardizing the document language.

Use A Template

A pre-defined format helps deliver information in a consistent and structured manner.

Describe Findings

What to include:

- Unique identifier
- Title
- Description
- CVSS score (and/or severity)
- Attack scenario (with the ability to reproduce)
- Recommendations (?)

Proofread!

Ask another pair of eyes for a peer review (it can be an AI, of course).

Automation And Tools

Prerequisites

The choice of a "technology stack" depends on where your pentesting source data comes from.

What's On The Market?

- Tools for pentesting teams (DefectDojo, Dradis, Faraday)
- Various generic reporting tools (Ghostwriter, Serpico, etc)
- Content and format linting tools
- AI-assisted tools for proofreading (like Grammarly)

Thank You

Q&A / Feedback