How to Write a Pentesting Report – With Checklist

Written By
Chad Kime

Published October 31, 2023

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.

We explore the art of writing effective penetration testing reports in the sections below:

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.

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.

Also read:

- 7 Types of Penetration Testing: Guide to Pentest Methods & Types
- Penetration Testing Phases & Steps Explained

8 Common Sections to Include in a Pentest Report

Every penetration test will be unique because each organization's IT infrastructure, security stack, application code, website APIs, and vulnerabilities will be a unique combination. However, the usability of the report depends on a writer's ability to take the unique information and organize it into an expected format clearly and concisely.

Some components of a pen test will be mandatory and must be present to provide value. Other components are nice to have because they help to improve the value of the report to stakeholders. The table below lists key information on eight common sections found in a typical pentest report, which we'll go into in more detail below.

Section	Must / Nice to Have	Order in the Report	Order in the Drafting	Level of Detail	Level of Technical Info
Executive Summary	Must Have	1	5	Low	Low
Key Findings	Must Have	2	4	High	High
Engagement Summary	Must Have	3	1	Low	Low
Full Pen Test Results	Must Have	4	2	Medium	Medium
Ratings & Risk Score	Nice to Have	5 (appendix)	Pre-draft	n/a	n/a
Vulnerability Details	Nice to Have	6 (appendix)	Pre-draft	Medium	High
Full Testing Procedure	Nice to Have	7 (appendix)	3	High	High
Acronym Appendix	Nice to Have	8 (appendix)	Pre-draft	n/a	n/a

Executive Summary

Unless an organization is extremely technical and focused on security, the executives of the company that make resource allocation decisions will generally not understand most of the key findings of a pentest report. They may know they have a network, but not u stand how firewall rules protect that network.

The executive summary contains similar sections as the rest of the report, but in summary form: key findings, engagement summary, and overall penetration test results. Where possible, tables, charts, and graphics should be used to help quickly convey the findings by severity rating, items to address immediately, etc.

The executive summary will generally be placed first in the pen test report, but written last once all of the other findings have been compiled and drafted. This is perhaps the most critical section of the report since the non-technical executives will likely determine future budgets for vulnerability correction and pentesting needs.

Key Findings

As this is the most important section for the technical team, it is placed as the second major section of the report.

For every unique vulnerability identified, the pen test report writer will create a vulnerability report. All major vulnerabilities will be listed and detailed within the key findings section, with backup information that explains:

- **Vulnerability name**, standardized if possible
- **Location** of the vulnerability (list of systems, apps, etc.)
- **Technique** used to find the vulnerability
- **Proof of concept**, or an explanation of how the vulnerability was actually exploited or might have been exploited
- **Likelihood of exploitation** within the context of the organization and current trends
- **Potential impact** of the exploit directly to affected systems and indirectly if there are cascading effects to security or operations
- **Overall risk assessment** based on the nature of the vulnerability, ease of exploit, likelihood of exploit, and impact to the security stack and the overall business impact
- **Recommendations**, at a high level, to eliminate or mitigate the vulnerability

While this appears second in the report, it will be one of the last sections drafted, as the Key Findings will be extracted from the Full Penetration Test Results.

This section should contain only the high-risk vulnerabilities that need to be addressed. Low-risk vulnerabilities can be listed in a table or graph in this section but details on less important vulnerabilities should be left for the Penetration Test Results section.

For clients that do not wish to use the penetration testing team for remediation, a high-level list of potential remediations should be used that explains possible solutions. A short recommendation such as “upgrade to version 10.x” will often be sufficient, but should also consider the context of the business environment.

For example, a Windows XP machine maintained to run critical industrial equipment will be highly vulnerable and easily exploited. However, a recommendation to simply replace the old computer with a Windows 11 machine will be useless to the client that can only use Windows XP with that equipment.

If the client has contracted for remediation or if this is an internal penetration testing report, recommendations may need to be quite involved and include prices for various options, timelines, and labor requirements. In some cases this might merit a separate Remediation Section.

Engagement Summary

The Engagement Summary can be the first section written because it comes from the statement of work. This section provides the context for the full penetration test results to follow and should outline both the original terms of engagement as well as any added requirements or limitations introduced in the course of the testing.

This section should include:

- The scope of the testing, including IP addresses, systems, applications, exclusions, etc.
- The timeline, including dates of testing and times (if limited) for testing specific resources (example: only test the web application between 10pm and 11pm weekdays)
- Security defenses tested
- Assumptions
- Standards applied to testing, such as PTES standard for networks, OWASP for applications
- Compliance standards considered in the testing

Full Pen Test Results

The Full Pen Test Results section includes all details for all testing performed. Instead of focusing on vulnerabilities, this section will focus on a system-by-system and test-by-test review of the penetration testing process.

This section can be very long as it will contain many details. It will typically be written as a draft or as notes early in the process and pen testers can put raw notes and screenshots here initially.

If the section seems too long, some repetitive information for non-critical vulnerabilities can be moved to the appendix. For example, if a test was performed on all 1,500 endpoints in an organization and was blocked by the local firewall, it would be better to give this test a name and show that the endpoints passed the test. The details of how this test was performed can be moved to the Full Testing Procedure Details Appendix.

Ratings & Risk Score Appendix

When assigning priority to vulnerabilities, most penetration testing companies use a standardized method and score to determine a rating or risk score (numeric or qualitative). This section in the appendix should explain the system for the client and will usually be written in advance as a standardized section of all pen test reports.

Vulnerability Details Appendix

For each vulnerability found, the vulnerability can be explained in detail in this appendix.

For example, most non-technical readers will not need to know the details of a cross-site scripting (XSS) vulnerability and many technical teams already know what they are.

A full explanation may not be needed and therefore not included in the main sections of the pentest. However, some might find more details helpful and thus an appendix can be considered. Since many vulnerabilities are standardized, this section can also be prepared in advance for the most common vulnerabilities expected in the pentest.

Full Testing Procedure Details Appendix

As noted above, some testing will be repetitive and if they do not result in any discovered vulnerabilities the tests may not be interesting. However, some technical teams and some compliance auditors will want to see the methodology performed for each test and would appreciate a detailed appendix section.

Acronym Appendix

Security and IT use an enormous number of acronyms for technologies, vulnerabilities, protocols, etc. This appendix should explain each acronym used in the report to help eliminate any confusion and misunderstanding. For electronic copies, the acronyms used elsewhere in the report could use internal document links directly to this appendix.

3 Factors For Effective Penetration Test Reports

For a pentest report to be effective, the results must be useful and provide value to all levels of readers, from executives to hands-on technicians.

Pentest report writers must keep these three factors in mind:

- **Penetration test objectives** that will vary at different levels of the organization
- **Useful pentest results** must be provided to extract value
- **Tips and cautions** to maximize the value of the report

Penetration Test Objectives

When authorizing a penetration test, an organization seeks to test their existing security controls for the systems authorized for testing. To deliver value on this investment, the penetration test writer must display the professionalism and competence of the testers clearly, both through the results of the test and the effective communication of the results.

The penetration test report content must reflect the objectives of a diverse set of stakeholders:

- **Executives and board members** will want to see value for their investment and need a clear and understandable non-technical summary
- **Technical teams** will want clear, detailed, and actionable information that can be used to remedy discovered vulnerabilities
- **Compliance and legal** teams will need penetration test results that clearly show how the organization satisfies their compliance obligations
- **Penetration testers**, of course, want to demonstrate the quality of their skills and the satisfaction of the objectives of the testing process

Penetration test results will be used to determine resource allocations, remediation requirements, justify the acquisition of new cybersecurity tools, and determine the urgency of corrective action. Usable reports enable these goals efficiently and effectively.

The key factors for usability are: clear presentation, client customization, and standardized ratings.

Clear Presentation

The pen test report writer must consider how to clearly present:

- Importance of Key Findings
- Overall findings
- Recommended Remediations
- Technical details
- Tested systems and methods used

Often tables and graphics help for easy digestion of information and should be used frequently. Similarly, a pen test report should be written as clearly and concisely as possible for clear and quick understanding.

Client Customization

Although key findings will typically be listed by severity and overall findings will tend to be listed by system, a pen test report should be customized to the needs of the client. For example, in a large enterprise, there may be separate groups responsible for networks and for application development. This type of organization will likely want reports with completely segregated key findings and overall results organized by team responsibility.

Standardized Ratings

A simple good / bad rating will not convey enough information, but will be equally as useful as an overly complex matrix of, say, three categories of eight possible ratings levels. To be most usable, ratings need to mirror ratings systems familiar to the technical teams.

The Common Weakness Enumeration (CWE) list developed by MITRE or scores based on the Common Vulnerability Scoring System (CVSS) will be familiar to all technical staff and are not too difficult to explain to executives. While these scores will lack the context of the business or active exploitation efforts, using standardized ratings as an initial base will typically be appreciated and easily understood.

Tips and Cautions

The main purpose of pentesting is to locate and remediate vulnerabilities before an attacker can exploit them. However, there are adjacent issues related to compliance and confidentiality that need to be considered for testing and reporting.

Compliance Penetration Tests

Generic pentests can check for vulnerabilities, but not necessarily touch on all elements to verify compliance. Some compliance standards require specific tests on specific systems and penetration testers should be told of such requirements in advance.

Likewise the pen test report should reflect any compliance needs and specifically demonstrate the pen test results against specific compliance standards, either as the core of the penetration test results or within related appendices. The report should specifically demonstrate that the security for systems or processes protecting regulated data have been tested as required and the results of those required tests.

Penetration Test Confidentiality

Confidentiality is key to security. Yet a thorough penetration test result will include many confidential details (IP addresses, security tool settings, application code, etc.) that would seriously harm an organization if exposed.

Confer with the client to determine the distribution needs for the report. If necessary, offer an edited or redacted version of the report that removes confidential information for broader distribution to non-privileged stakeholders (customers, vendors, affected executives, etc.). The client should also be consulted to determine the need for compliance-specific reports that contain only the pen test results for systems and assets touching the regulated data.

If delivering reports electronically, consider encrypted or technologically restricted distribution (specific-user only permissions, etc.). Physical reports should be numbered and tracked.

Pentest Report Checklist

Pentest Report Checklist		
Complete?	**Step**	**Item**
	Plan	Engagement Summary Draft
	Plan	Verify any compliance requirements (testing, reporting)
	Plan	Verify any confidentiality requirements (special drafts, special distribution, redacted versions, etc.)
	Plan	Full Pen Test Outline*
	Plan	Ratings & Risk Score Draft (optional)
	Plan	Vulnerability Details Draft (optional)
	Plan	Acronym Appendix Draft (optional)
	Tech Details	Verify all required tests are performed
	Tech Details	Obtain supporting documentation for all tests
	Rough Draft	Draft initial full pentest results
	Rough Draft	Move unnecessary testing information to Full Testing Procedure appendix
	Key Findings	Extract critical vulnerability findings to a draft of the Key Findings section
	Key Findings	Draft the Executive Summary
	Revise Draft	Create graphics and tables to simplify communication of key information
	Revise Draft	Double-check technical details with pentest technicians
	Revise Draft	Confirm critical documentation present to illustrate tests performed, vulnerabilities found, risk assessments, and recommendations
	Revise Draft	Convert all notes to formal text
	Revise Draft	Convert technical jargon to clear, everyday English – particularly for the Executive Summary
	Proof	Check grammar, spelling
	Proof	Check formatting, tables of contents, footnotes, etc.

*The full pentest outline prepares the document with all of the systems and tests to be performed. This outline can enable pentesters to place their documentation directly within this document, or for pentest report writers to use the outline as a checklist to avoid missing any technical details.

5 Examples of Pentest Reports

There are almost as many different types of penetration test reports as there are systems to test. Fortunately, many penetration testing reports have been made public and can be found in a variety of resources. Two key repositories with hundreds of reports can be found at Pentest Reports and the public-pentesting-reports GitHub repository for JulioCesarFort.

Most published reports focus on application security testing which can be published for open source projects or older applications without disclosing dangerous secrets. Penetration tests for network security require redaction or changing the information to hide IP addresses and security measures that likely continue to remain in place.

- **Application Code Audit:** Kudelski Security code review provides an effective Issue Summary List and supporting technical details section.
- **External IP Address Penetration Report:** 7ASecurity pentest on an minivpn implementation provides quality findings and recommendations, but lacks a useful executive summary to determine the results at a glance.
- **Internal Network Pentest:** Rhino Security network assessment using open source nmap and nessus tools includes an attack narrative to help convey the significance and potential business impact of server message block (SMB) protocol issues.
- **Industrial Control System Network:** Redacted pentest on Next Generation Power, Electric, and Water on an ICS subnet demonstrates a good use of graphics and formatting to aid in communication.
- **Social Engineering or Phishing Test Report:** The Volkis phishing campaign report provides good process details, but lacks graphical representation of the findings to reinforce easy understanding of the executive summary.

Pen Test Report FAQ

What Is The Difference Between Internal and External Penetration Test Reports?

The biggest differences between internal and external penetration testing reports will typically be the formality. Internal penetration testing will often be conducted by employees of an organization and external pen testing will be conducted by third parties contracted for the work.

Third parties need to demonstrate more value and will often have more polished reports to demonstrate value. However, internal reports still need to accomplish all of the same goals and contain useful information for all readers so the key sections (executive summary, key findings, engagement summary, full pen test results) need to be present and the report must also be usable.

What is the Difference Between Application, Website, Infrastructure, and Physical Penetration Test Reports?

There is no real difference between different types of penetration test reports even for different penetration testing methods and the type of assets tested. The evidence and technical details for findings will be completely different, but the method, common sections, elements, and factors for success for different types of penetration test reports will be the same.

Bottom Line: Reports Are the Final Pentesting Product

Penetration testing plays an increasingly important role in assessing the health of security systems protecting organizations of all sizes. However, without an effective penetration test report, the investment in time and resources may be wasted, even with a quality penetration test assessment. Penetration testers must master the art of clearly presenting their results if they want their hard work to be appreciated.

Further reading:

- Penetration Testing vs Vulnerability Scanning: What's the Difference?
- 7 Best Penetration Testing Service Providers
- 7 Best Penetration Testing Tools & Software
- 8 Best Vulnerability Scanner Tools & Software

Previous article

Weekly Vulnerability Recap – October 30, 2023 – Citrix & Cisco Haunted by Vulnerabilities

Next article

Multi-Tenancy Cloud Security: Definition & Best Practices

Chad Kime

eSecurity Planet lead writer Chad Kime covers a variety of security, compliance, and risk topics. Before joining the site, Chad studied electrical engineering at UCLA, earned an MBA from USC, managed 200+ ediscovery

Table of Contents

Top Cybersecurity Companies

1 Ready1

2 Semperis

See Full List

Get the free newsletter

Subscribe to **Cybersecurity Insider** for top news, trends & analysis

Enter an email

By signing up to receive our newsletter, you agree to our Terms of Use and Privacy Policy.

Sign up

Related Articles

Microsoft Defender vs Bitdefender: Compare Antivirus Software

PRODUCTS May 27, 2025

Bitwarden vs Dashlane: Comparing Password Managers

NETWORKS May 14, 2025

9 Best DDoS Protection Service Providers in 2025

PRODUCTS March 31, 2025