001.6- The pentesting report

Introduction

The pentesting report is arguably one of the most important documents that come from a pentest. Do not be afraid to spend a significant amount of time to make this document shine and make sure that you use templates. Make your own template based on those you can find online as an example and remove what you do not need and add what you certainly have to.

Most topics of a report are general but there can be some differences depending on the client’s requirements and the type of test. For example, we won’t include a network scan result if we are only supposed to test a web application.

I will mark the items that are required according to me but of course, you can interpret this as you wish, you are the pentest expert.

First page [REQUIRED]

Describe metadata about the document.

Logo:

Version: x.y DRAFT/REVIEW/FINAL

Client: RatInc

Version header [REQUIRED]

In here, you will include a small table indicating the status of the document, who will review it and the dates.

Version	Status	Author	Reviewer	Reviewed
0.1	DRAFT	Wesley Thijs	Uncle Rat	NOK - See remarks
0.2	DRAFT	Wesley Thijs	Uncle Rat	OK - Send to client
0.3	CLIENT REVIEW	Wesley Thijs	Rat Inc - Auntie Rat	OK - Please add remarks
1.0	FINAL	Wesley Thijs	Rat Inc - Auntie Rat	OK - Signed

Who is who [REQUIRED]

Note down for both parties who the people are which should be contacted.

The XSS Rat

Wesley Thijs – Founder and pen-tester – Info@thexssrat.com

Testy MacTest – Pen-tester – test@thexssrat.com

info rat – Pen-tester – Info@thexssrat.com

RatInc

Foundy mcFound - Founder

Claus Shawb = COO

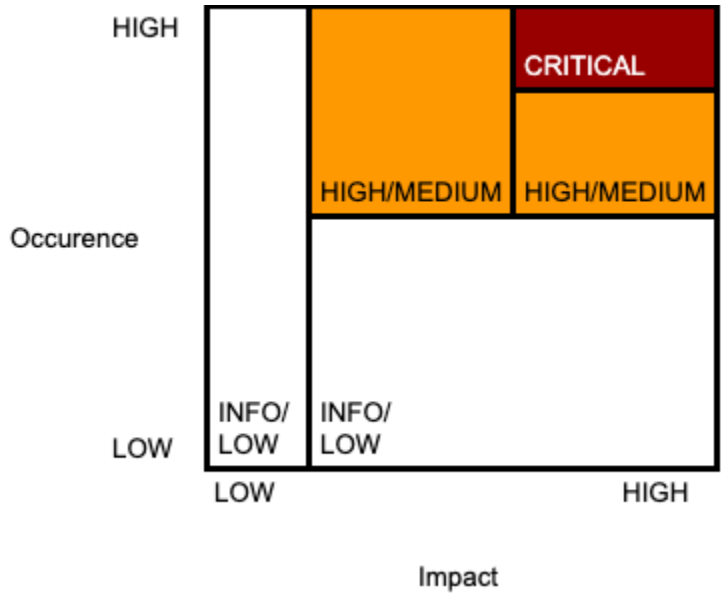
Leonardo dicaprio - Developer

Madonna - QA

Shakira - Just like her hips, her architecture work does not lie

Methodology[REQUIRED]

Don’t just write down that you followed the OWASP top 10, describe the phases of a pentest and how you will go about it.



Make sure you also explain how you come to your impact and risk assessments instead of just dropping an unknown classification on your client.

Always keep in mind the client's classification may differ from the one you give to a vulnerability. The client is always right in this case if you have advised them properly. You have to keep in mind that companies might be bound to budgets and their core business might differ from what you are used to.

Network scan [ONLY IN CASE OF NETWORK OR ORGANISATIONAL PENTEST]

Include your full Nmap and vulnerability scan results here. You might opt to put these results in an appendix so as to not clutter the report.

Findings[REQUIRED]

For every finding, try to complete the following template as well as possible:

IMPACT - Title

Make sure your title is concise, managers have to talk about your issues in a board room so make sure the titile says what is required in a short sentence.

Description

Shortly describe the issue, even though you will go deeper into the issue later. This will help anyone who is reading the issue to give context to what is going on.

Pre-condition

In case there is a pre-condition, you need to note it here. For example:

- Admin account available
- MiTM proxy such as burp suite

Steps to reproduce

When I explain to people what to type here, I always give them the example of having explained to a kid how to make a sandwich. It’s something you know how to do since you found the vulnerability and now you have to explain it to someone who does not know what to do.

It really pays off to spend some more time getting your steps in order since it might prevent the issue from being sent back and forth because the engineers might not be fully up to speed.

Be as detailed as possible but stay relevant to the case and only note the steps that would have caused the issue, try to eliminate all the variables so it’s easier for the engineers to figure out what is causing the issue.

Expected result

What is supposed to happen, for example:

“The user is supposed to get an error message”

Actual result

What really happened, for example:

“User was able to access invoices that he had no rights to”

Reference

Reference the CVE, CWE or OWASP top 10 item here if possible

Mitigation steps

As the security expert, you might be able to give some pointers as to how to fix the issue at hand. For example:

“Access control should be centralized in an authorization module that can be called upon instead of implementing the methods that already exist, with a chance to make a mistake.”

Impact

Include a section that explains the impact of the vulnerability based on the clients core business. Remember that you only give estimations and that the client can give a different weight to a vulnerability. Their core business might differ from your core intentions.

Metrics

Give you client an overview of the vulnerabilities you found, their compliance to the OWASP top 10 (if applicable) and an overview of the budget.

Critical	3
High	6
Medium	10
Low	4
Informational	22

Total hours spent testing: 322,5

Estimated hours: 350

OWASP compliance

Aa API1:2019 Broken Object Level Authorization	Pass	Date

Aa API1:2019 Broken Object Level Authorization	Pass	Date
API2:2019 Broken User Authentication	Pass	
API3:2019 Excessive Data Exposure	Pass	
API4:2019 Lack of Resources & Rate Limiting	Fail	
API5:2019 Broken Function Level Authorization	Pass	
API6:2019 Mass Assignment	Pass	
API7:2019 Security Misconfiguration	Fail	
API8:2019 Injection	Fail	
API9:2019 Improper Assets Management	Pass	
API10:2019 Insufficient Logging & Monitoring	Fail	

Conclusions

You should always give your client a general overview of the health of their system. Be concise but complete and give an unbiased opinion. You might be outraged that their Cisco firewall is a bit outdated but in reality, it might only form a mild security risk. Be realistic and honest and make sure the client knows what they are in for by reading this short summary.