001.4- The elements test plan

Revision history

This is a simple table, displaying the current and past versions of the document. (See example) It also displays the current state of the document (Draft, approval, final) and can contain some comments. This is not required but I always include it, it gives an easy overview of the current state of the document and who the author of that state is. Sometimes, the draft will be written by someone different than the final version for example.

Target audience

Use this section to indicate who the customer’s representatives are. Use direct names and ask your customer to who the report and plan should be sent. Don’t just send it out without checking as that would constitute a security vulnerability in itself.

Document goal

You always have to give a description of the purpose of this document. Remember that while it might seem obvious to you because you deal with documents like this all day, your client might not be as familiar as you with the standards and documents from our lovely profession.

Project description

This is a functional description of the project itself, not of the pentest. Your pentesting description will come later but for now, we have to give a short overview of the functionality of our application under test.

Glossary

Any terms that you use throughout the document which might be a bit harder to explain such as OWASP or MiTM poxy should go in here.

Objectives

Here, we describe what we hope to achieve with the pentest. As you might know by now, there are many different types of pentests and we have to ensure we describe the objectives so our client can easily review them and make sure we are both in line.

Methodology

In here you can give the client an overview of your tactics and your ways of attacking. Usually the level of coverage is also described in here and the phases of your pentest.

Recon >> Scanning >> Gaining access >> Maintaining access >> Covering tracks

is an example, you can describe each item in more detail and make sure your client understands what types of attacks you are going to be performing on their infrastructure.

Roles and responsibilities

Describe both on your side what team members are going to be partaking in this pentest and also what people to contact at the client's end. This makes it easier for pentesters to know who to contact in case they run into issues and also helps the client get an overview of who will be testing on their network.

Scopes of the tests

In here, try to describe as completely as possible what can (in scope) and can not be tested. This is important as it will avoid any discussions later on.

Assumptions

If you are making any assumptions during your test, for example, if the firewall is disabled you will “assume the attacker already managed to bypass the firewall”.

Test entry and exit criteria

Whenever you start testing, you might need certain things such as VPN access or specific accounts. Those are entry criteria and should be noted so the client knows what is expected of them.

Similarly, if anything can halt testing such as being blocked by Cloudflare for example, you have to note this as well so your client can know what to avoid and how to help you best.

Toolset

As you might imagine, your client might not be pleased with just any tool being run on their networks and while you are the expert in this manner, the client still does need to know what is going to happen after you commence testing. It’s a small extra to note down all the tools you will use and it will put the clients’ minds at ease.

List of deliverables

List all the deliverables that go alone with the project together with a date when they should be delivered. I usually include the following:

- Test plan
- NDA
- Notice of testing
- Test report
- Project debriefing

But you are free to add your own of course.