ISSAF Methodology
Analysis and Critical Evaluation

Florent Gontharet

Penetration Testing

University of Abertay Dundee

MSc Ethical Hacking

2015

Table of Contents

ABSTRACT

Introduction

Pentesting now represents a huge amount of security services. It consists in assessing the existing environment in order to find and fix weaknesses or security vulnerabilities. In order to conduct a complete and accurate pentest, methodologies are used, we are going to analyse the Information Systems Security Assessment Framework (ISSAF) methodology, from the Open Information Systems Security Group (OISSG).

Background

A methodology is important, as it provides a clear list of all aspects and assets to be assessed. It allows managers and administrators to plan and prepare the assessment.

Methodology

The document has been synthesised, analysed, and evaluated on the planning, the management, the legal and ethical aspects, each taking the support, guidance, and advices provided, as criteria.

Conclusion

The conclusion shows a long document, addressing to both managerial and technical public. The methodology is extremely detailed, making the version of the document an important point, as it has to be up-to-date to include new tools and technologies.

The different criteria and aspects have been entirely covered, however the verbosity of the document can lead more experimented pentesters to less detailed methodologies.

INTRODUCTION

Penetration testing has become a huge part of security. It allows an organisation to assess the existing security controls in place, in order to identify weaknesses, and reduce risks and threats, as well as vulnerabilities.

In order to conduct a complete and accurate pentest, a various amount of aspects have to be taken apart and analysed, based on the environment, the technologies, the architecture, the list can be continued. In order to give consistency to a test, it is important to not forget any of those aspects.

Methodologies have been developed in order to address the issue, giving clients an overview of the tests to be conducted, the aspects covered... In the other hand, it gives guidelines and scenarios for pentesters to follow, and make sure no aspect has been left aside during the assessment.

The ISSAF methodology will be critically analysed and evaluated. The choice of the ISSAF has been made because it is open-source and peer-reviewed.

BACKGROUND

As pentesting grows, companies have to understand what services the require, what test they need, what assets are vulnerable or what threats they can face. All those points have to be understood by both the pentesters' manager and the client, in order to address the client's request and needs. The use of a methodology for penetration testing provides consistency to the test and the results (Kang, 2008).

Also, a methodology should address both the technical and managerial people, a the first ones are going to conduct the tests, and the second need to know what is going to be conducted. However, their needs are different, as the managerial do not need the technical details in example.

The ISSAF is a framework provided by Open Information Systems Security Group (OISSG), a not-for-profit organization based in London.

The document gives assessments, strategies, as well as check-lists, in order to improve information security. As a framework, it can be integrated in the business life cycle. Its role is to secure infrastructures by assessing existing security controls.

It is known to give lists of the most common tools, that is a usually good point for community and help available (Shrestha, 2012).

METHODOLOGY

SYNTHESIS

First of all, the methodology itself counts two parts: the methodology, and the explained methodology.

It represents one of the particularities of the ISSAF methodology: it is separated in a managerial and a technical part. The managerial approach addresses the challenge in order to suits the needs of administrative employees, without overloading the document with technical aspects. In that managerial focus, we can find the three phases that makes the ISSAF methodology:

- The pre- assessment describes the planning and the the preparation of the test. The legal aspect is clearly explained and the main lines of the arrangements are given;
- The assessment covers the different tests that are going to be conducted, nothing technical, however, the methodology, aims and objectives of each and every test is given. At total, 9 steps are exposed in non-technical terms:
    1. Information Gathering
    2. Network Mapping
    3. Vulnerability Identification
    4. Penetration
    5. Gaining Access & Privilege Escalation
    6. Enumerating Further
    7. Compromise Remote Users/Sites
    8. Maintaining Access
    9. Covering Tracks;
- The post- assessment, last part, addresses some guidelines for the report writing, the reporting, and the destruction of all artefacts;

The second part, exposes the explained methodology, for the technical teams. Also, we do not find the three parts from the managerial plan, here is only presented the assessment itself, with the 9 steps covered before.

In order to explain them, each main step is first fully presented:

- Description, establishing a link with the last step, giving some informations and summary about the tools, techniques and such;
- Aim/Objective, giving the intentions and weaknesses to be tested;
- Process, a detailed list of the different steps, joined by technical data such as protocol names and ports, packet flags, sometimes with schemas.

The technical part also gives lists of tools to perform the different tasks, and a full guide of each technical manipulation, with a table grouping a short description, examples and results, analysis, countermeasures, and finally some remarks. Guidelines, approaches, points of views are widely shared, as well as scenarios and examples.

ANALYSIS

Now that we had an overlook of the document, we can analyse its content. The content is separated in two main parts, both addressing a different part, managerial or technical. This plan follows the same principle of the abstract in a technical report, addressing a quick look of each part, with the main points and conclusions. It makes the document clear, readable and understandable by non-technical people, answering the management and legal issues, as well as the arrangements that have to be established before the test. The dialogue with the client is approached, and the different tasks are presented.

Regarding the technical part, it is extremely detailed, with a lot of guidelines, advices, links between tasks themselves, and it gives the pentester explanations and test criteria for each, leading to a complete and accurate assessment. The 65 points, distributed in the 43 pages counted into the technical part represent a deep approach, including in tools and focuses.

EVALUATION

First, the planning is covered in the pre-assessment part of the managerial plan, making the document valuable for any manager in order to plan a pentest. Support, guidance, and advice are given for the managers.

The management has its own part, grouping all valuable information together, making the navigation in the document easy, leaving the manager with a comprehensible document, still linked to the technical part, but the content is not presented the same way, and with the same goal. Managerial problems, such as risk/control assessment, or legal issues are addressed. Advices are given, such as the advancement and conclusions of the different tasks, helping the manager to plan and understand or avoid issues (such as legal ones).

Regarding the methodology itself, it provides a clear sequence of tasks, with a complete overview, giving a disciplined framework, important in order to conduct a complete and accurate test. The connections between the tasks gives consistency, as well as the real life scenarios. Support, guidance, and advices are most of the content, helping the tester to fully understand the test and the controls to be tested.

CONCLUSION

In conclusion, we have seen the different aspects the ISSAF methodology covers, we find the main steps of a penetration testing, its approach makes it clear for anyone to understand. The different aspects are all covered, and issues have been addressed to provide a complete methodology.

The scenarios, and the amount of details however represent a huge maintenance in order to assimilate new updates, tools, or technologies. The OISSG claims it to be broad, up-to-date, and to include tools, best practices, as well as administrative concerns.

Among the Internet, the ISSAF is also described as “infancy”, or even “outdated” (Ali And Heriyanto, 2011). If tools and scenarios can evolve, and force the ISSAF user to stay up-to-date, steps and guidelines however are not changing everyday. A huge amount of technical data remains unchanged, and can helps in the process of understanding a new version of a protocol, as it usually is. Also, as an open-source document, it is maintained and new versions are published.

But mainly, the ISSAF is well known to provide a high value position about assessing existing security controls (Shrestha, 2012), and to connect tasks between themselves (Pandya, Year unknown). For a beginner pentester, it provides a goldmine, however trained pentesters will probably want to turn themselves to the OSSTMM, another methodology, that gives less examples, and more bullet-lists, in order to keep the content to a smaller volume.

REFERENCES

1. Ali And Heriyanto. 2011. BackTrack 4: Assuring Security by Penetration Testing.

[online] https://www.packtpub.com/books/content/backtrack-4-security-penetration-testing-methodology [accessed on April 23, 2015]

2. Kang. 2008. About Effective Penetration Testing Methodology. Journal of Security Engineering.

[online] http://www.sersc.org/journals/JSE/vol5_no5_2008/8.pdf [accessed on April 22, 2015]

3. Pandya. Year unknown. Penetration Testing and Its Methodologies.

[online] http://groups.hcon.in/uploads/1/8/1/9/1819392/hga_bhashit_pandya_-_pentest_methodologies.pdf [accessed on April 22, 2015]

4. Shrestha. 2012. Security Assessment via Penetration Testing: A Network and System Administrator's Approach.

[online] https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha-masterthesis.pdf [accessed on April 22, 2015]