Vulnerability Scanning with OpenVAS

Laboratory Report in EDA263/DAT641 Computer Security

Author 1
Author 2

Group XX

Version no: 0

February 6, 2014

Contents

1 Introduction **1**

2 Description of OpenVAS Setup **2**
2.1 Port Scanning 3
2.2 Fingerprinting 3
2.2.1 Service Fingerprinting 3
2.2.2 Remote Host Fingerprinting 3
2.3 Vulnerability Scanning 3

3 Results **4**
3.1 Port Scanning 4
3.2 Fingerprinting 4
3.2.1 Services 4
3.2.2 Remote Host 5
3.3 Vulnerability Scan 5

4 Discussion **6**

5 Conclusion **7**

References **8**

A Report from OpenVAS Vulnerability Scanning **9**

1 Introduction

This section shall introduce the reader to the subject addressed by the report. It should include a description of the purpose of the report, i.e., a formulation of the problem to which the report provides an answer. Try to motivate the reader to keep reading your report to know more about vulnerability scanning and OpenVAS.

The last paragraph should consist of a "roadmap" of the report, e.g., The rest of the paper is organized as follows: Section 2 provides...

General Notes about the report:

The report should be self-contained and descriptive. It is not allowed to use the lab-pm as a reference. You may read and use information from lap-pm, but do not copy text from any reference.

The purpose of the report is to train your skills in technical writing. So try to make it well-written and well-structured. In each section, it is not enough to only present the results. Try to be descriptive, do some research and elaborate on the results.

If you need information on LaTeX, [2] is a good place to start...

2 Description of OpenVAS Setup

This section should include a brief explanation of how the architecture of OpenVAS and a description of the setup of the scanned network. Try to find some references about OpenVAS and vulnerability scanning in general and write briefly:

• Why scanning is a useful method? What are the types of vulnarability scanning?
• What do we expect from the scanning results?
• How to perform it by OpenVAS?

Note: Do not forget to add references at the end of the report and refer to them in the text here.

This section should also describe the scans you are considering, including the chosen NVT families used (and possible exception or specific NVTs chosen) with their settings and parameters (in each step below). Explain in each step:

• Why you choose the different NVTs and the chosen configurations?
• What are the aim of the different scans and why did you make the different choices? For example, why did you only scan specific ports in your port scanning. Give details and motivations.

References to figure should be included in the text, e.g., "In Figure 1, the network setup is described. . . "

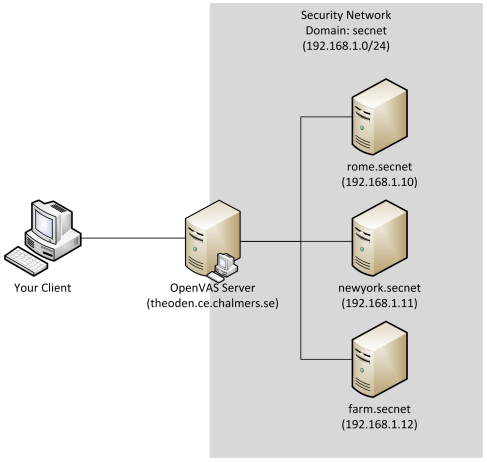

Figure 1: The laboratory network setup

2.1 Port Scanning

text, figures, and tables if needed. Figure captions are below of figures, and Table caption should be above them.

2.2 Fingerprinting

text, figures, and tables if needed

2.2.1 Service Fingerprinting

text, figures, and tables if needed

2.2.2 Remote Host Fingerprinting

text, figures, and tables if needed

2.3 Vulnerability Scanning

text, figures, and tables if needed

3 Results

Describe your results and findings. Tables should be commented in text, e.g., Table 1 shows the open ports that were found by OpenVAS. Table texts are above of table.

3.1 Port Scanning

Comment the information of the table in the text. Make sure that the caption numbers are correct.

Table 1: Information about open ports

Port Number	Service Name	Service Task	Suggestions

3.2 Fingerprinting

3.2.1 Services

Comment the information of the table in the text. You may extend the table with more entries you found interesting. Make sure that the caption numbers are correct.

Table 2: Service fingerprint

Service	Version
Telnet	
FTP	
SSH	
SMTP	
WWW	

3.2.2 Remote Host

Describe your findings about the remote host, e.g., Host Operating system, architecture, etc.

3.3 Vulnerability Scan

Describe your findings. Use OpenVAS vulnerability scan report, you may include report in appendix if you think it would be useful.

4 Discussion

Discuss your findings in different parts. Comment the information of Table 3 in the text. You may extend the table with more entries you found interesting. Make sure that the caption numbers are correct.
• Elaborate on what needs to be done to improve the security.
• Support your decisions with facts and recommendations from OpenVAS, such as severity of problem.
• Compare your recommendations to the recommendations you made in Assignment 1.

Table 3: Summary of vulnerability scan recommendations

Service Name	**Problems**	**Suggestions**

5 Conclusion

Present your conclusions and recommendations. Propose a strategy for keeping the system secure. A computer is constantly exposed to various threats. Propose a strategy for keeping a networked computer up to date with security. List a few actions that should be done regularly to keep the computer secure.

References

[1] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr. "Basic Concepts and Taxonomy of Dependable and Secure Computing". In: *IEEE Transactions on Dependable and Secure Computing* 1.1 (2004), pp. 11–33. DOI: 10.1109/TDSC.2004.2.

[2] *LaTeX - Wikibooks, open books for an open world*. URL: http://en.wikibooks.org/wiki/LaTeX.

Please use Vancouver/IEEE style for your referencing. For more information please check: http://www.lib.unimelb.edu.au/cite/ieee/index.html. References can easily be managed with the program JabRef.

A Report from OpenVAS Vulnerability Scanning

Possibly include your report from your full scan with OpenVAS.