Vulnerability Scanning with OpenVAS

Laboratory report in

EDA263/DIT641 Computer Security

Author 1

Author 2

Group Number:

Chalmers University of Technology

Gothenburg, Sweden 2015

Version no.: 0.0

Table of Contents

[1. Introduction 1](#_Toc348958490)

[2. Description of OpenVAS setup 2](#_Toc348958491)

[2.1 Port scanning 2](#_Toc348958492)

[2.2 Service fingerprinting 2](#_Toc348958493)

[2.2.1 Service fingerprinting 2](#_Toc348958494)

[2.2.2 Remote host fingerprinting 2](#_Toc348958495)

[2.3 Vulnerability scanning 2](#_Toc348958496)

[3. Results 3](#_Toc348958497)

[3.1 Port scanning results 3](#_Toc348958498)

[3.2 Fingerprinting results 3](#_Toc348958499)

[3.2.1 Service fingerprinting 3](#_Toc348958500)

[3.2.2 Remote host fingerprinting 3](#_Toc348958501)

[3.3 Vulnerability scanning results 3](#_Toc348958502)

[4. Discussion 5](#_Toc348958503)

[5. Conclusions 6](#_Toc348958504)

[**References** 7](#_Toc348958505)

[**Appendix: OpenVAS Vulnerability scan report** 8](#_Toc348958506)

# 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.}

# 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…”}

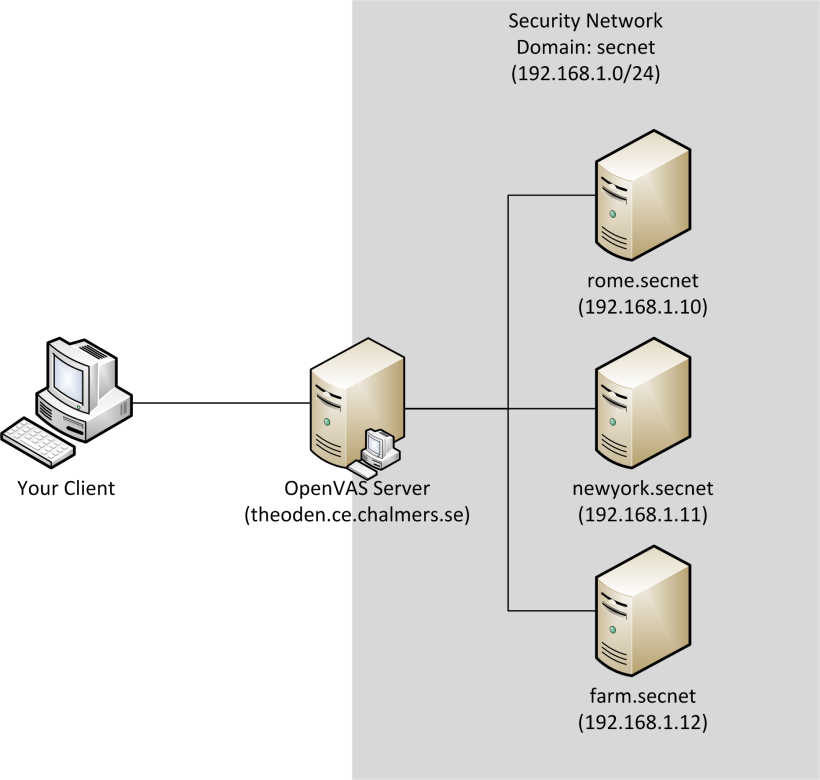


Figure 1: The laboratory network setup

## Port scanning

{text, figures and tables if needed}

## Service fingerprinting

{text, figures and tables if needed}

### Service fingerprinting

{text, figures and tables if needed}

### Remote host fingerprinting

{text, figures and tables if needed}

## Vulnerability scanning

{text, figures and tables if needed}

# 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.}

## Port scanning results

{Comment the information of the table in the text. Make sure that the caption numbers are correct, table size fits in the margin and well structured.}

Table 1: Information about open ports

|  |  |  |  |
| --- | --- | --- | --- |
| **Port number** | **Service name** | **Service task** | **Suggestions** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Fingerprinting results

### Service fingerprinting

Table 2: Service fingerprint

|  |  |
| --- | --- |
| **Service** | **Version** |
| **telnet** |  |
| **ftp** |  |
| **ssh** |  |
| **smtp** |  |
| **www** |  |

{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 size fits in the margin and well structured.}

### Remote host fingerprinting

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

## Vulnerability scanning results

{Describe your findings. Use OpenVAS vulnerability scan report. You may include the report in appendix if you think it would be useful, but it is just as a reference for details for interested readers. So you should explain here your findings and provide interesting results that you found in the report and comment on them.}

# Discussion

{Discuss your findings in different parts. 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.

* 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** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Conclusions

{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**

{Use the Vancouver/IEEE style for referencing. For more information please check: <http://www.lib.unimelb.edu.au/cite/ieee/index.html>

For example:

[1] W. Stallings and L. Brown: Computer Security, Pearson 2012, ISBN: 978-0-273-76449-6.

**Appendix: OpenVAS Vulnerability scan report**