Mittuniversitetet
MID SWEDEN UNIVERSITY

Laboratory Assignment: Host-Based Intrusion Detection

Daniel Bosk*

hids.tex 2169 2015-01-14 22:37:01Z danbos

Contents

1 Introduction

This laboratory exercise will cover the topic of intrusion detection systems (IDS). An IDS monitors the activity of a system and alert the administrator if any potential threats are detected. This laboratory work will focus on host-based intrusion detection systems (HIDS), in particular OSSEC[1].

2 Scope and Aim

After completion of this assignment you will

- Have an understanding for the functionality of a host-based intrusion detection system.
- Be able to analyse functions of an intrusion detection system.

This laboratory assignment will cover the open source HIDS OSSEC.

[1] URL: `http://www.ossec.net/`.

3 Reading instructions

Before starting this assignment you should have first read chapter 10 "Banking and Book-keeping" in *Security Engineering* [1] followed by section 17.4 in *Computer Security* [2]. Then you should read chapters 2-4 in *OSSEC HIDS: Host-based Intrusion Detection Guide* [3–5], covering how OSSEC works.

4 Assignment

This section covers the work to be done and the next section covers how it will be examined, and what to be done to pass.

Firstly you should install the OSSEC software. You can find it on URL

`http://www.ossec.net/`.

The installation procedure is documented both on the website and in [3], the instructions on the Web are of course more up-to-date.

Once the system is installed and up-and-running, you should select one of the features it was designed for, e.g. log analysis, real-time alerts, agentless monitoring, file integrity checking, active respone, among other things. You will now evaluate this feature and prepare a demonstration of it. This demonstration should present at least the following:

- What is interesting about this feature?
- How you evaluated the feature.
- A demonstration of its use.

5 Examination

As you will prepare a demonstration, this will be presented for the class (check the course schedule for the date of this presentation). You are required to have some slides to present your selected feature and your evaluation, and then of course the live demonstration. You should give your presentation (demonstration), it should be at most 15 minutes long.

References

[1] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: `http://www.cl.cam.ac.uk/~rja14/book.html`.

[2] Dieter Gollmann. *Computer Security*. 3rd ed. Chichester, West Sussex, U.K.: Wiley, 2011. ISBN: 9780470741153 (pbk.)

[3] Andrew Hay, Daniel Cid, and Rory Bray. "Installation". In: *OSSEC HIDS: Host-Based Intrusion Detection Guide*. Syngress Publishing, Inc., 2008. Chap. 2. URL: `http://ossec.net/ossec-docs/OSSEC-book-ch2.pdf`.

[4] Andrew Hay, Daniel Cid, and Rory Bray. "OSSEC HIDS Configuration". In: *OSSEC HIDS: Host-Based Intrusion Detection Guide*. Syngress Publishing, Inc., 2008. Chap. 3. URL: http://ossec.net/ossec-docs/OSSEC-book-ch3.pdf.

[5] Andrew Hay, Daniel Cid, and Rory Bray. "Working with Rules". In: *OSSEC HIDS: Host-Based Intrusion Detection Guide*. Syngress Publishing, Inc., 2008. Chap. 4. URL: http://ossec.net/ossec-docs/OSSEC-book-ch4.pdf.