DT116G Network Security

Laboratory Assignment: Intrusion Detection

Daniel Bosk[*]and Lennart Franked[†]

lab_IDS.tex 1262 2013-09-05 08:10:53Z 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. In this course we are going to focus solely on Network Intrustion Detection Systems (NIDS).

Before starting this assignment you should have completed the laboratory assignment covering GNU Privacy Guard (GPG).

2 Aim

After completion of this assignment you will

[*] E-post: `daniel.bosk@miun.se`.

[†] E-post: `lennart.franked@miun.se`.

- Demonstrate ability to detect and possibly prevent attacks on a network.

This laboratory assignment will cover the open source NIDS Snort.

3 Reading instructions

Before starting this assignment you should have read chapters 10 to 13 in Stallings [1]. You should also read chapters 1, 2.1, 2.4, 2.5, 2.9, 3.1-3.4 in the Snort documentation [2].

4 Tasks

This section contains the task that you must perform in order pass this laboratory assignment.

4.1 Installation

Visit the Snort webpage and download the Snort installation files together with the Snort rules package.

`http://www.Snort.org`

Once installed add the Snort rules files to your working installation. Select one rule and use appropriate methods to test and see if the rule works.

When you have confirmed that the rules are working, You shall solve *one* of the scenarios given below. Consult the documentation [2] for help on how to solve it. Note that not all scenarios can be solved solely with the help of Snort.

4.2 Scenario 1: Online Exam

In a computer networking course that is given at Mid Sweden University, the students take exams by logging in to a specific web site and access the exam there. You have been given the task to, with the help of Snort, create a series of rules that will alert the teacher if a student is accessing another web page during the exam. Since the students do not want to be disturbed during the exam, it is of vital importance that the rules will not result in any false positives. You can use Cisco Netspace if you have an account there, otherwise, use any online test available on the internet.

4.3 Scenario 2: Snort as an IDPS

You are tired of all the reconnaissance attacks that your server have been the victim of lately, therefore you decide to with the help of Snort, block all traffic from a destination that have performed such an attack (you can self decide what specific type of reconnaissance attack you have been the victim of).

4.4 Scenario 3: Snort Notification

You are running a server that is connected to the public network and would like to get notified when this server is a victim of an attack without having to go through the system logs. You will therefore configure Snort to notify you either using email or by SNMP whenever a potential attack is detected. (You can self decide what these attacks can be). As an optional task, you also would like to create statistical data on how often your server is being attacked. The data must be presented in such a way that you can, per attack, see how many times per hour and per day this attack occurs. It should be represented either in a text file that can easily be parsed to a spreadsheet program, or in a format readable to for example MRTG.

5 Examination

The following results must be handed in.

- Give a short summary of your installation process, including adding and testing of the rules.
- Give a detailed description on how you solved the scenario, Include your rule(s), together with a detailed description of how it (they) works, also a description of how you tested it and the resulting entry in the log file.

5.1 Bonus

You can receive a 2 point bonus on the first exam in this course by solving Scenario 3. To get the bonus, the passed version of the laboratory assignment must be submitted in time.

References

[1] William Stallings. *Network security essentials : applications and standards.* Pearson Education, 5 edition, 2013. ISBN 978-0-273-79336-6. International Edition.

[2] The Snort Project. Snort users manual, May 2013. URL `http://s3.amazonaws.com/snort-org/www/assets/166/snort_manual.pdf`.