Network Security Summer 2015 Exercise 4

TECHNISCHE UNIVERSITÄT DARMSTADT

Prof. Dr.-Ing. Matthias Hollick
Secure Mobile Networking Lab — SEEMOO
`https://www.seemoo.de`

Goal

The goal of the first part of this exercise is to give you a brief understanding of Intrusion Detection Systems (IDS) and the Snort rule language. The second part shall familiarize you with basic port scanning and service identification techniques.

Deadline

The hard deadline for this exercise is **Wednesday 10th June, 2015, 23:00:00**. Late submissions are subject to the following penalty: (1) up to 1 day late: you will obtain 50 % of the achieved points; (2) up to 2 days late: you will obtain 25 % of the achieved points; (3) more than 2 days late: you will obtain zero points.

Bonus system

We decided to install a credit-based bonus system in our course. We will hand out credits in certain exercises if you (the students) deliver first-rate performance. Within the relevant exercises we will document the detailed requirements to obtain the bonus. Throughout the entire course 280 credits can be obtained in our bonus system. If you score at least 230 credits, you are eligible for a 0.7 grade bonus in the final exam. If you score between 190 and 229 credits, you are eligible for a 0.3 grade bonus. Below 190 credits we will not issue any bonus.

In this exercise you can earn up to *85 bonus credits* (45 bonus credits for Problem 4.1, and 40 bonus points for Problem 4.2).

How to solve this exercise

In this exercise you are asked to write a couple of rules to be used with the Snort intrusion detection system (Problem 4.1) and to perform information reconnaissance with nmap (Problem 4.2).

Please hand in your solution in a single text file (plain ASCII or PDF) using the known naming convention *ex04_lastname_firstname*. Other formats will not be accepted.

Problem 4.1 Intrusion Detection with Snort

Snort Setup

You will need to setup your own Snort system before you can work on the exercise.

Install Snorby Spsa. Download the *Snorby Spsa* security distribution from `http://sourceforge.net/projects/spsa/files/` and run the live CD. You can either install the system on your local computer or on a virtual machine to do all the work. Just follow the setup assistant provided in the "Advanced Menu."

As a virtualization platform we recommend VirtualBox from Oracle (`http://www.virtualbox.org`). Other tools like VMware or Parallels should work as well, but we will not provide support for them if you encounter any issues.

NetSec setup script. Once you have your basic system up and running you should download and execute our Network Security setup script from our servers. You can reach the command prompt using the "Advanced Menu" and "Quit" option or by switching to another console using the *Alt+F2* key combination. Please note that the keyboard still has a US layout. A full key map can be found at `http://en.wikipedia.org/wiki/Keyboard_layout#United_States`.

Now execute using the following commands[1]:

[1] `--no-check-certificate` is required since the wget version shipped with Snorby Spsa does not support SNI. This is a good example on how to undermine transport layer security ;-)

```
wget https://seemoo.de/netsec-ids --no-check-certificate
chmod +x setup.sh
./setup.sh
```

At the end of the setup process you are asked to choose your time zone which should normally be *Europe/Berlin* and your keyboard layout which should normally be *Generic 105-key (Intl) PC - Germany - Romanian keyboard with German letters, eliminate dead keys*.

A new Snort configuration file will be installed under */etc/snort/rules/netsec.rules*. You can use this file to test all of your Snort rules. For testing purposes a web server is installed and running at `http://<YOUR_SERVERIP>`.

There is also a web based front end to view all events triggered by Snort. The GUI can be found at `https://<YOUR_SERVERIP>:8080`. Use the user name *Snorby* with password *admin* to log in. Please make sure you use HTTPS and not HTTP, otherwise it will not work.

Note that you have to restart the Snort service every time you change a configuration or rule. Use the following commands to restart Snort:

```
/etc/init.d/snort stop
/etc/init.d/snort start
```

Now you are ready to start the exercise.

Problem 4.1.1 Detecting Content (Bonus: 10 credits)

The exam for Network Security is stored on the HTTP Server. We would like to monitor any access from the outside to be sure that only authorized people access the exam download page. Unfortunately the file name of the page can change from year to year, so you have to set a filter for the content of the HTML file. Therefore, the main headline of the restricted page will always contain the string "Network Security Exam" followed by the study term.

A sample file can be found under */netsec/exam2015.html* on the web server.

Please write a Snort rule that sends out a notification (low severity) to the administrator whenever a HTML document containing a headline in the format mentioned above is accessed. The event category should display "NetSec Exam Page Access" in the Snorby front end. Make sure your rule is not triggered by accessing the *index.html* page.

Problem 4.1.2 Detecting File Types (Bonus: 15 credits)

The actual exam file is also stored on the server. It is a PDF file with a changing file name as well. You can find an appropriate file under */netsec/exam2015.pdf*.

Please write a Snort rule and use the classification "NetSec Exam Download" in the front end with a medium severity level to notify the administrator whenever an exam PDF document is accessed on the web server.

Problem 4.1.3 URI Filtering (Bonus: 20 credits)

Finally, all exam solutions of the last three years are stored on the server as well. The filename of each solution follows the naming convention *exam<YEAR>_solution-v<VERSION>.jpg* where *<YEAR>* is the year of the exam and *<VERSION>* is a 3-digit number. The first NetSec exam was 2011, thus, *YEAR* can be any integer number between 2011 and 2015. *VERSION* can be any number with 3 digits (000–999). A sample exam solution matching the above naming convention can be found on the web server under */netsec/exam2015_solution-v215.jpg*.

As the web server is also used for other exams you are asked to write a Snort rule to match all file names of the format mentioned above which are stored in a `netsec` subdirectory anywhere on the server and *which actually exist*. Any non-existent file names or file names not following the above naming convention should not be matched.

You are asked to write a Snort rule to notify the administrator whenever a server access, matching the above mentioned rule, occurs. As the download of an exam solution is highly critical you will need to send an alert (high severity level) whenever such a document is accessed. Please use the event category "NetSec Solution Access" to distinguish such access from other severe events.

Additional hints

Under certain conditions, the Snorby web interface does not work properly. If you are sure your rules should work but do not show up in the Snorby web interface, the following tips should help:

- If you want to look up some details about Snort, you can find the manual here: `http://manual.snort.org/`
- Line breaks in the .rules file must be in UNIX-format.

- Check if you inserted all your new classifications to `/etc/snort/classification.config`.
- Avoid local caching, e. g., use *Ctrl+F5* (or similar) to refresh the page with your browser.
- Make sure that line 16 in `/etc/lighttpd/lighttpd.conf` (`mod_compress`) is commented out with an '#'.
- If your alerts do not show up in the web interface try to start Snort manually: Disable database logging (comment out `snort.conf:273`) and add "`output alert_fast: stdout`" below. After this you can start Snort with the following command: `snort -c /etc/snort/snort.conf -k none -P 10000`
- Check if Snort listens on the correct network interface. If not, you can start Snort manually with the correct interface as follows: `snort -i eth1 -c /etc/snort/snort.conf`
- If you encounter bugs or problems, keep calm, this is expected to happen.

Problem 4.2 Reconnaissance

For this problem, we provide a server at 130.83.194.149 which will be online until the deadline. Please note that the server is reachable from inside and outside the university intranet. However, we recommend to open a VPN connection into the university network first if you want to work from an outside computer.

For solving the problem, we recommend the nmap port scanning tool which is freely available at `www.nmap.org`. You may, however, also use a different port scanner of your choice. *Important: This exercise is not an invitation for hacking attempts on the provided server or the university network!*

Problem 4.2.1 Basic Scanning (Bonus: 20 credits)

First, find out the DNS name of the provided server using a tool of your choice. Then, perform a port scan and answer the following questions:

a) What operating system is the server running? Justify your assumption.

b) Is the server running an SSH daemon? If so, provide the public host key.

c) Which ports are open on the server? Are any "unusual" ports open, i. e., ports that are normally not used by common protocols?

d) Which services are running on the server? Which ports belong to which services? Justify and explain your findings.

e) Which applications are used to provide the services? What are their version numbers?

Try to find as much basic information about the server and the services it provides as you can. Play around with the options of your port scanner to fully utilize its capabilities. Have an extra look at services that are *hidden*, i. e., that are not in a standard configuration in an attempt to hide them or intentionally provide misleading information.

Problem 4.2.2 More Advanced Information Retrieval (Bonus: 20 credits)

Have a closer look at the provided services. Is there any public information you can retrieve?

Collect tokens. We have distributed a set of *tokens* across the services. A token is an alphanumeric string that is clearly labeled as a token for this exercise. If you find a token, you will see that it is one. Record it in your exercise solution together with the commands and utilities you used to obtain it.

Leave us a message. Some services also invite you to leave a message. If you see such an invitation, save a string to the server and report it in your exercise solution. Do not enter your student ID or any other confidential information as it will be visible to your fellow students. This is **not** an invitation to jam the server's hard disk with garbage, a short string is fully sufficient. Please ensure that only you can claim the messages by using some type of hash (and tell us what you have hashed).

Find the misconfiguration (1 credit). One of the services is configured in a very insecure manner. Find this misconfiguration and tell us how to correct it. Propose the corresponding entries for the configuration file. (By misconfiguration we do not mean configurations that enable you the access to tokens or the creation of messages.)

The number of credits you receive depend upon the number of tokens you find and number of messages that you leave behind on the server. *Hint: If you need an account somewhere, try the user "anonymous" with the password "netsec". If you need a database name, try "netsec".*

Important: Please put all your tokens into a text file "lastname_firstname_tokens.txt" and your messages into "lastname_firstname_messages.txt". Without these files your tokens and message will not be accepted!