جامعة بيرزيت

BIRZEIT UNIVERSITY

Faculty of Engineering and Technology
Department of Computer Science

Opponent Report (No.10)

Laith Marzouka	ID: 1160827
Khaled Awashreh	ID: 1150393

Supervisor: Dr.Hafez Barghouth

Spring Semester 2019

Date: May 21, 2019

1) What is the topic?

UNIX OS Security.

2) Does the paper contain a clear abstract about the objective or even is that mention clearly in the introduction?

The abstract is very general and does not specify what exactly they are going to go through. However, the introduction standing along with the literature form a solid basis about the core of the report which is the Unix based OS.

3) In a few sentences summarize what the paper is about?

The paper talks about the Unix based Operating system layers and how the OS tries to establish its security by implementing some methods such as hiding the passwords file from the public, making the owner of the files in charge of its permissions for all other users, and giving one person the root the ability to take control of everything and have permissions on any files in the system. The paper also gives guidance about how to change permissions and what are the privileges for the root.

4) From your point of view does the author follow the scientific way to write a paper?

Yes, it follows the way of a scientific paper. However, that does not mean that the content does so. For example, the abstract was way too general and not clear.As well as, the conclusion wasn’t very impressive. Furthermore, the future work part was not included.

5) Is there any conclusion that is mentioned clearly at the end and if there is one can you summarize it using your own words.

It is clear enough. It mostly emphasizes that implementing a safe system needs a lot of work and the capability to take into consideration any vulnerable possibility.

6) Is it a logical conclusion that really can be derived from the previous content or not? Justify?.

The conclusion is not really body-related, it does not sum up what was discussed in the body. No real offered solutions to increase security potential.

7) What are the strong points in the paper project?

-The report is simple and organized.

-The methods of pointing out to the information are clear.

- Examples of applications with commands were given.

8) What are the weaknesses of the project?

-Fails to give a clear abstract.

-The conclusion is unrelated to the discussion.

-No personal touch on how to improve the system or even their opinion about how secure it is.

-Overall fuzziness and incomplete explanations.

-No real solid data, merely ideas and concepts.

-Weak hierarchy of ideas and concepts

-

9) Write questions (at least three questions).

1- “always log in as a normal user and then use the “su -“ (switch user) command” (Page ‘8’). Why is that, not clear?

2- Isn’t there any way to avoid events written on the log file? Plus, if the attack is done from the attacker by using the root/any authorized client, log file records are useless for identifying the criminal.

3- What is exactly a single-user mode, how does it work?

4- How can an attacker forcibly invoke the system to restart? Is that type of attack detectable?

10) If you are allowed to give a grade to this paper with a scale from A TO F what you will give and what is the criteria for the given grade. (how did you decide).

C. While there was some hierarchy of ideas and concepts, in many areas it felt like several topics/ideas weren’t discussed or clarified just merely mentioned. the material is not comprehensive enough and the language can be bit confusing and fuzzy It should have contained more deeply topics about how exactly the system deals with intruders and suspicious files.

Good command examples were given.

The content of the body is solid. In contrast, the abstract and conclusion were not very clear.