World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:16, No:08, 2022

TACTICAL: Ram Image Retrieval in Linux Using Protected Mode Architecture's Paging Technique

Authors : Sedat Aktas, Egemen Ulusoy, Remzi Yildirim

Abstract : This article explains how to get a ram image from a computer with a Linux operating system and what steps should be followed while getting it. What we mean by taking a ram image is the process of dumping the physical memory instantly and writing it to a file. This process can be likened to taking a picture of everything in the computer's memory at that moment. This process is very important for tools that analyze ram images. Volatility can be given as an example because before these tools can analyze ram, images must be taken. These tools are used extensively in the forensic world. Forensic, on the other hand, is a set of processes for digitally examining the information on any computer or server on behalf of official authorities. In this article, the protected mode architecture in the Linux operating system is examined, and the way to save the image sample of the kernel driver and system memory to disk is followed. Tables and access methods to be used in the operating system are examined based on the basic architecture of the operating system, and the most appropriate methods and application methods are transferred to the article. Since there is no article directly related to this study on Linux in the literature, it is aimed to contribute to the literature with this study on obtaining ram images. LIME can be mentioned as a similar tool, but there is no explanation about the memory dumping method of this tool. Considering the frequency of use of these tools, the contribution of the study in the field of forensic medicine has been the main motivation of the study due to the intense studies on ram image in the field of forensics.

Keywords : linux, paging, addressing, ram-image, memory dumping, kernel modules, forensic
Conference Title : ICCESAD 2022 : International Conference on Computer Engineering, Software Applications and Design
Conference Location : Istanbul, Türkiye
Conference Dates : August 16-17, 2022