Abstract

Live forensic investigation is conducted when the computer system is turned on whilst the data is gathered in a forensically sound manner, from the physical memory, in the form of evidence. As time progressed, criminals have been developing methodologies by which live analysis could be defeated. One such method implemented by the criminals is that of a rookit being installed on the victim’s machine. A rookit can be dangerous, and very risky to deal with from an investigator’s point of view, because it has the power to subvert the kernel of an operating system. This paper presents, how easy it is for a criminal to thwart the process of live forensic investigation by downloading and installing free software tools; needing, no prior knowledge of the windows 7 operating system’s kernel, and how frustrating it would be for the investigator to examine the computer system and make a valid forensic report. Thus, making live analysis a daunting task for the forensic investigator on field. Finally, a mathematical formula is derived for detecting the presence of hidden processes in the memory.

References

- C. Pogue, C. Altheide and T. Haerkos (2008), UNIX and Linux Forensic Analysis DVD Toolkit, Syngress Publishing.
- Harlan Carvey (2005), Windows Forensics and Incident Recovery, Addison Wesley, Burlington.
- Bill Blunden (2009), The Rootkit Arsenal: Escape and Evasion, Jones and Bartlett Learning, Texas.
- Internet Engineering Task Force, url: https://www.ietf.org/rfc/rfc3227. txt
Index Terms

Computer Science  Operating Systems

Keywords

Anti-Forensics  Digital Forensics  Computer Forensics  Memory Forensics  Live Response.