Malware is malicious code that tends to take control of the system remotely. The author of these codes drops their malicious payload on to the vulnerable system and continues to maintain access to this system at will. In order to unravel and establish the ability of rootkit to hide system network interface, we developed a network model, and implementation of this model was carried out on four notable live rootkits. Our results show the ability of the four rootkits to hide the system network interfaces, which are being used by the attackers to gain access and communicate correctly with the compromised system.