Abstract

Network security deals with two types of communities - black hats and white hats. The era of security has come when the white hats are not only interested in defending the networks but are keen to make fool of the black hats. Looking at the other side of the mirror, the black hats have also evolved new methods of breaching the security. The work in this paper is based on implementation of low-interaction and high-interaction honeypots along with the deployment of honeywall gateway. Honeywall gateway acts as reverse firewall that allows all type of traffic (both good and bad) to enter the system to facilitate analysis and learning. Honeywall gateway is the heart of the work that is involved in capturing, controlling, and analysis of data. The captured data is further categorized on protocol and port basis. The methodology used can be summarized into three steps: • Monitoring the attack traffic • Analyzing the attack type and method • Responding to the attacker to capture in depth information. The work is intended to analyze the attacker’s activities once it is logged and captured by honeywall and accessed through the walleye interface.

References
Implementation of High Interaction Honeypot to Analyze the Network Traffic and Prevention of Attacks on Protocol/Port Basis

- Alimerkaj, Gilmand, "Development of AIT's HoneyNet", Athens Information Technology, Center of excellence for Research and Graduate Education.
- "Configuracion del Honeywall CDROM", http://www.youtube.com/watch?v=HZiylQ_tdgo
- "Development of the Honeyd virtual Honeypot", www.honeyd.org
- "HoneyPot/honeyd tutorial part 1, getting started", http://www.travisaltman.com/honeypot-honeyd-tutorial-part-1-getting-started
- "Hping", www.hping.org
- "Instalacion del Honeywall CDROM", http://www.youtube.com/watch?v=sBLIHFc64jM.
- "Installing Honeyd 1. 5c And Arpd 0. 2 Under CentOS 5 (With gcc 4. x)", http://www.howtoforge.com/installing-honeyd-1.5c-and-arpd-0.2-under-centos-5-with-gcc-4.x
- "Know Your Enemy: GenII Honeynets", The Honeynet Project.
Implementation of High Interaction Honeypot to Analyze the Network Traffic and Prevention of Attacks on Protocol/Port Basis


Index Terms

Computer Science  Security

Keywords

honeyd  attacks  honeypots  honeynet gateway  honeywall  sebek