Abstract

Security in computing world is a serious issue and must be handle with utmost care, hence the need to always protect and secure our networks as more and more business are been conducted through the internet. The expansion of the World Wide Web has given unlimited access to attackers to prey on ignorant administrator who lacks basic knowledge of network security. Vulnerabilities in common security components such as firewalls, security patches, access control and encryption are inevitable, so hackers take advantage of these loopholes to break into computer networks. This paper presents the result of a research that was carried out using a medium interaction honeypot, a virtual machine ware workstation, snort software and entropy-based model for capturing, analyzing and detection of malicious traffic targeted at the network. A ring topology network of three system was design using virtual machine work station, a Snort software was installed on all the three machine to capture traffic on the network and entropy-based mathematical analysis was conducted on the traffic to detect attack/malicious traffic. The entropy $H(x) = -\sum_{i=1}^{N} N_i \log_2 (P_i)$ where $P_i = N_i/S$. $N$ is a set of positive integer that represent the total number of server on the network, $n_i$ represent the size of the traffic in bytes and $S$ represent the total length of the traffic that
constitute the traffic. The result of the research work shows detection of malicious traffic and also limit the rate of denial of service targeted at the network.

References

- Eric Peter, epeter(at)wustl(dot)edu and Todd Schiller, tschiller(at)acm(dot)org (A project report written under the guidance of Prof Raj Jain). A practical guide to honeypot.
Design and Implementation of a Medium Interaction Honeypot

- National Institute of Standards and Technology (NIST) "Guidelines on firewalls and firewall policy"; January 2002
- Nor Badrul Anuar, Omar Zakaria, and Chong Wei Yao University of Malaya, Kuala Lumpur MY Honeypot through Web: The emerging of security application integration.
- P. Dewan, P. Dasgupta, and V. Karamcheti. "Defending against Denial of Service attacks using Secure Name resolution"; 2003
- Raifeeq Ur Rehman, 2003. Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID
- Saleh Ibrahim Bakr Almotairi. Using honeypots to analyse Anomalous internet activities.

- The Honeynet Project: Research alliance, http://www.honeynet.org, non-profit Honeypot research organization, 1999
- [LOBSTER] LOBSTER-Large-scale Monitoring of Broadband Internet
- A virtual Honeypot framework, Niels provos Google, Inc. niel@google.com

Index Terms

Computer Science  Security

Keywords

honeypot  security  Network  traffic & detection