Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.407 – 412

RESEARCH ARTICLE

Mitigating Risk Using Puzzle-Based Defense Technique to Improve Confidentiality

Ms. Sapna S. Khapre[1], Prof. Shrikant Ardhapurkar[2]
[1]M.Tech.-CSE, Smt. Bhagwati Chaturvedi College of Engg, Nagpur, Maharashtra, India
[2]CSE/IT Department, Smt. Bhagwati Chaturvedi College of Engg, Nagpur, Maharashtra, India

[1] sapnakhapre27@gmail.com; [2] shrikant.999@gmail.com

Abstract— ***A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. DoS attack is an attack that attempts to cause a failure in a computer system or other data processing entity by providing more input than the entity can process properly. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. To provide prevention against DoS attacks game theory is used. This is mainly owing to the several trade-offs existing in a flooding attack defense scenario. In this defense technique the resources can be used by legitimate users only by login with correct id and password and by solving puzzle correctly. The puzzle is generated randomly for each login. To improve the quality of service for legitimate user and also to improve confidentiality, puzzle based defense technique is used. With the help of puzzle based system we can avoid DoS attack.***

Full Text: http://www.ijcsmc.com/docs/papers/June2013/V2I6201397.pdf