Abstract

Cloud security has been an important area of research nowadays. The vulnerabilities of cloud system can be easily explored by any attacker and compromise these virtual machines to deploy DDoS i.e. Distributed denial of service attack which involves multi step exploitation, compromising virtual machines as zombies, low frequency vulnerability scanning and Lastly DDoS attack through the zombies. In Infrastructure-as-a-service (Iaas) clouds, detection of zombies is extremely difficult. Hence to prevent virtual machines to be compromised as zombies, a new system was proposed as Network Intrusion detection and Countermeasure Selection, Abbreviated as NICE. It uses countermeasures based on reconfigurable virtual network and uses attack graphs. This paper provides survey of techniques of NICE and countermeasures taken to prevent the machines from being compromised as zombies.


**Index Terms**

Computer Science Networks

**Keywords**

Network security, Intrusion detection, Countermeasure selection, Cloud computing, Attack graph, Zombie Detection.