International Journal of Information Security and Privacy
Volume 12 • Issue 1 • January-March 2018

Optimized Packet Filtering Honeypot with Snooping Agents in Intrusion Detection System for WLAN

Gulshan Kumar, Lovely Professional University, Punjab, India
Rahul Saha, Lovely Professional University, Punjab, India
Mandeep Singh, Lovely Professional University, Punjab, India
Mritunjay Kumar Rai, Lovely Professional University, Punjab, India

ABSTRACT

Wireless LAN networks are considered to be widely used and efficient infrastructure used in different domains of communication. In this paper, we worked on Network Intrusion Detection System (NIDS) to prevent intruder's activities by using snooping agents and honeypot on the network. The idea behind using snooping agents and honeypot is to provide network management in term of monitoring. Honey pot is placed just after the Firewall and intrusion system have strongly coupled synchronize with snooping agents Monitoring is considered at packet level and pattern level of the traffic. Simulation filtered and monitor traffic for highlight the intrusion in the network. Further attack sequence has been created and have shown the effects of attack sequence on scenario which have both honey pot and snoop agent with different network performance parameters like throughput, network load, queuing delay, retransmission attempt and packet. The simulation scenario shows the impact of attack on the network performance.

KEYWORDS

Agents, Honeypot, Intrusion, Monitoring, Security, Snooping

INTRODUCTION

As the usage of internet increases most commonly user tasks are accomplished through it and for this the concept of distributed applications or databases has been considerably grown at the peak to provide fast access. Due to this wide network number of intruders also increases. So, there is need to put some strong mechanism across the network to restrict unauthorised access and for this various network devices such as firewall and Intrusion Detection Systems (IDS) (Mohame, Idris, Shanmugum, 2012) have been developed to block variety of attacks/threats to the network through incoming connections. Intrusion detection is the process of monitoring and capturing the network traffic and events occurring in a computer system that is later used to analysing them for malicious activities and possible signs of incident which are violations or threats of violation of computer security policies, acceptable use of policies and standard security practices that is defined by system administrators. An intrusion detection system (IDS) plays an important role in a network to provide good security environment. It enables the administrators to detect suspicious packets, activities, network vulnerabilities and attacks. All network traffic can be observed with the help of IDS and t is

DOI: 10.4018/IJISP.2018010105

easy to detect as well as decode malicious traffic on a honey net (Li, Sun, & Zhang, 2011). and log some malicious packets at a centralized database.

The honeypot (Zhai & Wang, 2012) is an effective tool for observing and understanding intruder's methods, tactics, behaviour and motivations. A honeypot observes and suspects every packet that is transmitted to and from it, giving it the ability to collect and capture less noisy datasets for network attack analysis. However, they do not replace traditional security systems they provide extension to network security whose value lies in unauthorized or illicit use of that resource. Honeypot (Mairh, Barik, Verma & Jena, 2011) is an emerging technology with great network security potential that can be placed inside, outside of the network as well as deployed inside of the firewall. It is a trap set used to divert attackers and hackers away from critical resources for unauthorised use. It can also be used to study an attacker's methods and tools. It provides a large amount of valuable information that is used for analysis through which variety of attacks can be detected even working within an encrypted environment. All honeypot work (Mairh, Barik, Verma & Jena, 2011) same as they do not have any production value and they have no authorized activity so any interaction with honeypot is treated as malicious and unauthorized activity It acts as a warning tool which produce alarm if any malicious activity detected but it has risks associated with it such as firewalls being penetrated, encryption can be broken, failing of IDS sensors etc. Honey pot have many advantages such as small data sets which collect limited amount of information instead of gigabytes of data logging, reduced false positive for legitimate activity, catching false negatives for malicious activities, working with encrypted and IPV6 environment, highly flexible and simple, require minimal resources to capture bad activity. A generic implementation of honeypot has been shown in Figure 1.

Low-interaction honeypots (Spitzner, 2002) are used for production purposes that capture limited amount of traffic or information. The services offered by low interaction honeypot are basically emulated and allow operating systems with limited amount interaction for attacker. The activities used by attackers are limited to some extent of emulation that is offered by the honeypot. The advantages of low-interaction honeypots are that they are simple to manage and easier to deploy. In addition, the limited amount of emulation helps to reduce the potential risks for low interaction honeypot. However, experienced attackers can easily recognise a low interaction honeypot when they deal with them. High-interaction honeypots (Spitzner, 2002) are used for research purpose as they are more complex to deploy and manage. They involve real operating systems and applications by giving attackers real systems nothing there is emulated and no such restrictions are imposed on attacker behaviour in the order to find how attacker progress or execute in real time and this helps administrators to monitor or capture extensive details about the full extent of an attackers' methods. However, it is also possible that attackers might use this real honeypot system to attack other systems within the organisation. Therefore, strict protection policies need to be implemented accordingly. In the worst case, sometimes a network connection may be disconnected to prevent attackers from further penetrating the network and systems that are not under the reach of honeypot system.

Figure 1. Generic implementation of honeypot