IJRSET 2015 SPL Volume 2, Issue 9 Pages: 19-22

IJRSET

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

OVERVIEW OF INTRUSION DETECTION SYSTEM IN WIRELESS MESH NETWORK

[1] Mr. K. Khumaravel, MCA, M.Phil, [2] CCNA, (Ph.D), [3] Ms. V. Renugadevi,
[1] Head of the Department, [2, 3] Research Scholar,
[1, 2, 3] Department of Computer Science,
[1, 2, 3] Dr.N.G.P. Arts and Science College, Coimbatore.

Abstract:-

Intrusion detection is the process of detecting unauthorized traffic on a network or a device. Intrusion Detection Systems (IDS) are designed to detect the real-time intrusions and to stop the attack. An IDs is software or a physical device that monitors traffic on the network and detect unauthorized entry that violates security policy. Intrusion detection in wireless mesh networks (WMNs) is especially challenging and requires particular design considerations. In this paper we present various attacks in wireless network and some techniques to prevent from those attacks.

Keywords: - unauthorized, security policy, confidentiality, malicious actions.

1. INTRODUCTION

An intrusion is any unwanted activity either in the form of passive attacks or active attacks, which are used by the attackers to create undesired situation and harmful consequences for the user's confidentiality, network integrity or network resources availability.

In simple words, any set of actions that try to compromise the data integrity, then user's confidentiality or service availability can be termed as intrusion, while a system that attempts to detect such malicious actions of network or compromised nodes is called IDS.

owever, the security level of wireless networks can be enhanced up to certain limit by implementing IDS. The primary functions of IDS are to monitor users' activities, network behaviour and different Layers. A single perfect defence is neither feasible nor possible in wireless networks, As there always exist some architectural weaknesses, software bugs or design flaws which may be compromised by the intruders.

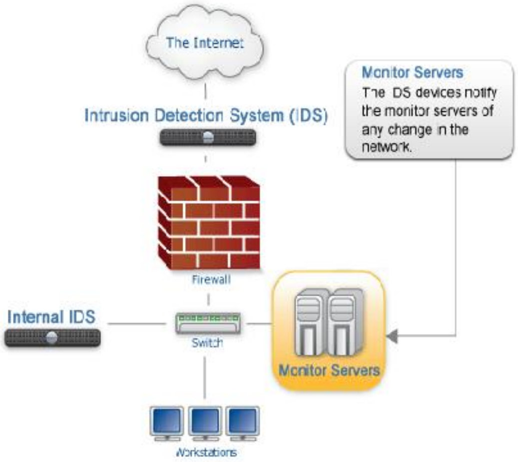
The Internet
Intrusion Detection System (IDS)
Monitor Servers
The DS devices notify the monitor servers of any change in the network.
Firewall
Internal IDS
Switch
Monitor Servers
Workstations

Figure.1 Intrusion Detection System

IDS is more critical in wireless networks which is viewed as a passive defence, as it is not intended to prevent attacks instead it alert network administrator about possible attacks well in time to stop or reduce the impact of the attack. The accuracy of intrusion detection is generally measured in terms of false positives (false alarms) and false negatives (attacks not detected).

2. TYPES OF MALICIOUS ATTACKS

Some of the possible attacks are summarized as follows:

Eavesdropping: Adversaries use electronic transmitting or recording devices to monitor Wireless communications to gain critical information. It is generally the first step in launching further attacks in wireless networks.

Traffic Analysis: Adversaries analyze traffic flows to deduce information from the patterns of wireless communication without cracking the security system of the wireless Communication system.

Radio Jamming: Adversaries transmit a high-power signal to disrupt or interfere with legitimate wireless communication.

Replay Attack: Adversaries may replay messages received from other nodes or received previously to disturb the functionalities of wireless networks.

Rushing Attack: Adversaries always forward route request packets more quickly than legitimate nodes in order to increase the probability that routes with attackers will be discovered rather than other valid routers.

Wormhole Attack: Adversaries build a wormhole tunnel between two end points Which are usually multi-hops away. The message recorded at one end point is relayed to the other end and re-broadcasted into the network, which fools the wireless nodes far from each other to believe they are neighbours.

Black hole Attack: An adversary node advertises itself as having the shortest path to the destination node whose traffic it Wants to intercept. By doing this, the malicious node can deprive the traffic from the source node.

Packet Dropping/Selective Forwarding: A compromised node may drop all or some of the messages that should be forwarded.

Packet Flooding: Adversaries may send a huge amount of useless information to the network through compromised nodes to disrupt wireless communication.

3. THE DETECTION TECHNOLOGIES

The few of the categories of the Detection technologies are, Network Based, Wireless, Network Behaviour Anomaly Detection and Host-Based.

A Network Intrusion Detection System (NIDS): This technology analyzes network traffic at every layer of the OSI model for suspicious activity.

Wireless local area network (WLAN): IDS analyzes wireless-specific traffic, including scanning for unauthorized users trying to connect to active wireless network components.

Network Behaviour Anomaly Detection: Network behaviour anomaly detection (NBAD) analyzes network traffic to identify anomalies that exists if any.

Host-based intrusion detection systems (HIDS): This technique is analyzes system-specific settings including security policies, log audits and software calls.

4. DETECTION TYPES

Few types of detections include Signature-Based Detection, Anomaly-Based Detection and Stateful Protocol Inspection.

Signature -Based Detection: An IDS can use signature-based detection completely relying on known traffic data and analyzes potentially unwanted traffic. It has a limited detection capability.

Anomaly-Based Detection: An IDS analyzes the traffic on the network and detects incorrect, invalid and abnormal IP packets hybrid or compound detection system combines both approaches. In essence, a hybrid detection system is a signature inspired intrusion detection system. that makes a decision using a hybrid model. This is based on both the normal behaviour of the system and the intrusive behaviour of the Intruders.

Stateful Protocol Inspection: An IDs that inspects traffic at the network and transport layer including the vendor specific traffic in the application layer for any malicious behaviour.

5. UNIQUE CHALLENGES OF WIRELESS MESH NETWORKS

Wireless Medium: The wireless medium is one of the major factors effecting intrusion detection. In wire Networks, traffic is forced to travel along links, and there are natural points of traffic concentration which are convenient locations for intrusion detection. This is not as valid in a wireless mesh network, particularly if it is entirely ad hoc. However there might be a backbone of fixed wireless routers. In that case, the traffic through access points should be monitored. In practice, this is difficult because access points typically do not have “SPAN ports” that mirror the traffic. Monitoring traffic by promiscuously eavesdropping on the radio medium is not ideal. Nodes in a wireless mesh network may have relatively short radio ranges (just long enough to reach the next node), so sensors are able to see only limited amounts of traffic. Multiple sensors need to be deployed around the entire network for a comprehensive view of traffic. Another difficulty presented by the wireless medium is the mobility afforded to no .As mentioned, mobile devices might travel to hostile environments. A mobile device without adequate protection could be physically compromised. Therefore, nodes in a wireless mesh network are more Vulnerable to compromise and cannot be entirely trusted even if their identity is authenticated.

Dynamic Network Topology: Again, the dynamic topology of wireless mesh networks means that there are no natural fixed points of traffic concentration which would be good choices for monitoring. A possible approach is to run IDS on certain hosts to monitor their local neighbourhood’s .However; a node can not be expected to monitor the same area for a long time due to its mobility. A node may be unable to obtain a large sample of data for accurate intrusion detection.

CONCLUSION

Confidentiality ensures that the data is only read by the intended recipients. An IDs analyzes the traffic on the network and detects incorrect.
invalid and abnormal IP packets hybrid or compound detection system combines both approaches.IDS is more critical in wireless networks which is viewed as a passive defence, as it is not intended to prevent attacks it alert network administrator about possible attacks well in time to stop Or reduce the impact of the attack using the above technique to prevent from attacks such as Black hole Attack, and so on..

REFERENCES

[1] Iftikhar Ahmad, Azween B Abdullah, Abdullah S Alghamdi —Comparative Analysis of Intrusion Detection Approaches‖, 2010 12th International Conference on Computer.

[2] T. Lunt, —Detecting intruders in computer systems, in Conference on Auditing and Computer Technology, 1993.

[3] Khan and et al “Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks”, The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[4] G. Cretu, J. Parekh, K. Wang, and S. Stolfo. Intrustion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks. In Consumer Communications

and Networking Conference, pages 635–639, Las Vegas, NV, Jan. 2006.

[5] Chen M., Kuo S., Li P., and Zhu M., Intrusion Detection in Wireless Mesh Networks, CRC Press, 2007.

[6] Northcutt S. and Novak J., Network Intrusion Detection, SAMS Publishing, 2002.