Detecting The Attack On The Distributed Mobile Notice Board Using Android

Keerthi Rajan, V. Visveswaran

Abstract: Intrusion detection system is the key component for ensuring the safety of systems and networks. There are a number of challenges facing by the intrusion detection; an intrusion detection system must efficiently find out the malicious activities in a network and must perform reliably to cope with the network traffic. This paper develops an advanced notice board system using android where the registered members can post their content and which can be seen by the entire member users. Here performing four kind of intrusion detection for the notice board; probe, dos, r2l and u2r detection. Layer based intrusion detection approach is used to detect the four attacks which has been mentioned before.

Index terms: Intrusion detection system, malicious activities, notice board system, probe, dos, r2l, and u2r.

1 INTRODUCTION

Intrusion detection is the method of detecting inaccurate, malicious, or anomalous activity [1]. Since the type and way of the attack is increasing day by day, for network administrators and security professionals, intrusion detection is one of the highest priority and challenging task. The task of an intrusion detection system is to inform the system or network administrators when it monitors the network traffic and malicious activity. Intrusion detection system not only monitors the system but also in some cases it can also react to malicious traffic by taking the actions such as blocking the user or source IP address. The intrusion detection system must be efficient and accurate in detecting attacks. The system must face so much challenges to become accurate, an accurate system cannot manage large number of network traffic and it may cause the decision making become slowly. We wish a system that detects maximum of the attacks. An intrusion detection system (IDS) monitors the system or network activities for anomalous activities and produces reports to a management station. There are two kinds of IDS; network based (NIDS) and host based (HIDS) intrusion detection system [2]. There are two other kinds of intrusion detection system (IDS); signature based and anomaly based depending upon the attack detection method. The already available patterns from previously known attack can train the signature based system. However the anomalous based system is trained by the non attacked or normal data collected when there is no malicious activity [3]. The signature based detection system worked same as a virus scanner, by searching for a known pattern for intrusion [4]. Anomaly based intrusion detection system detect any type of misuse, however the signature based system can only detect the attack for which a signature has previously created [5].

- *Keerthi Rajan, V. Visveswaran*
- *MTech, School of Engineering and Technology JAIN University, Asst.Prof, School of Engineering and Technology Jain University*

2. RELATED WORK

Intrusion detection has been start around since 1980's. Many systems have been implemented and a number of methods have been proposed to detect intrusion. Harve Deban [6] proposed a state based intrusion detection system. It includes security assessment tools such as Tiger and, COPS for host environments, and for network based environments Nessus, Satan and Ballistia. When a vulnerable application or a configuration error is present then these tools identify error states. Robust intrusion detection system using Layered approach with Conditional Random Fields [7] proposed a three layer system to ensure complete security through availability, confidentiality and integrity. This system can identify an attack once it is detected at a particular layer. Thus it can minimize the impact of an attack. To ensure the layers are linked together, share some features from previous layers. Ankita Gaur and Vineet Richariya [8] proposed a layered approach for intrusion detection using meta-modeling with a classification techniques. Classification is defined as a supervised learning algorithm in the machine learning process. Brajesh Patel [9] proposed a system using time based detection to identify a fast attack intrusion. Based on number of connections made in 1 second, this system can identify anomalies. This methodology implemented on a different set of real network traffic.

3. PARAMETERS OF PROPOSED SYSTEM

3.1 NETWORK ATTACKS

Network security consists of the techniques adopted by a network administrator to prevent and monitor misuse, gaining unauthorized access, unauthorized modification, or making impossible of access to a computer network and network resources. Network security is controlled by the network administrator. Network security consists of the authorization of access to data in a network. Users choose an ID and password or authenticating information that allows them access to information within their authority. This paper considers four types of attacks; probe, DoS, R2L and U2R attack.

3.1.1 Probe Attack

Probe attack is an attempt to collect information about a computer network for the malicious purpose of gaining its security controls. This paper considers four kinds of probe attack detection. That is, IP sweep, NMap (Network Mapper), port sweep and SATAN (Automated Network Vulnerability Scanner) attacks. IP Sweep is an address sweep performed

by sending a defined number of ICMP packets to different host by same source IP address within a defined time interval. The attacker then uncovering a host address to the target which has replied to the attacker. NMap (Network Mapper) attack can locate IP address in use, ports in use and controls the operating system in use. The port Sweep attack does not give a direct control by port scanning. To find which ports are available to launch various attacks is helping the attacker by port scan. It is finding an active port by sending a client request to a range of server port addresses on a host. SATAN is an automated network vulnerability scanner. It is used by both administrators and attackers to search for malicious activities on a network. For attacker to perform an attack is useful with the information provided by SATAN. 5 parameters are using to detect the Probe attack. The parameters are; duration (duration of the connection in number of seconds), protocol type (type of protocol), service (network service), flag (status of the connection), src_bytes (number of data bytes from source to destination).

3.1.2 DOS Attack

DOS (Denial of Service) are an attack in which the attacker makes some computing resources impossible to access. There are four kinds of DoS attack; back, LAND (Local Area Network Denial), Neptune and POD (Ping of Death) attack. Backdoor in a computer system is a method of securing unauthorized remote access to a computer, bypassing normal authentication, and so on. A LAND (Local Area Network Denial) attack is a DoS attack that locks up a system when sending a special malware packet to a computer. The attack involves sending a connection initiation packet (TCP SYN) to the target host's IP address as both source and destination. The result is machine reply to itself continuously. Neptune sending session establishment packet to generates a SYN flood attack against a network host. POD (Ping of Death) is a type of attack on a computer that sending a malformed or malicious ping to a computer. 9 parameters are using to detect the DoS attack. The parameters are; duration (duration of the connection in number of seconds), protocol type (type of protocol), flag (status of the connection), src_bytes (number of data bytes from source to destination), count (number of connection to the same host), dst_host_same_srv_rate (% of connection to the same service), dst_host_serror_rate (% of connections have SYN errors), dst_host_srv_serror_rate (% of connections to the same service and % of connections that have SYN errors), dst_host_rerror_rate (% of connections that have REJ errors).

3.1.3 R2L Attack

R2L (Remote to Local) attack occurs when an attacker who is capable of sending packets to a machine over a network, but who is not an authorized user on that machine and it generate some vulnerability to gain local access as a user of that machine. Here considering four types of R2L attack; guess password, IMAP (Internet Message Access Protocol), multihop and spy. Guess password is a type of password guessing attack and it consist of trying every possible combination, code or password. IMAP (Internet Message Access Protocol) allows different clients accessing the same mailbox at the same or different times when several clients simultaneously connected to the same mailbox, and can identify the state changes made by other clients. Multihop can be defined as the process of passing data from device to device using the most reliable communication links until the destination is reached. Spy attacker presence is typically hidden from the user and can be difficult to detect whenever spyware is used for malicious purposes. 14 parameters are using to detect the R2L attack. The parameters are; duration (duration of the connection in number of seconds), protocol type (type of protocol), service (network service), flag (status of the connection), src_bytes (number of data bytes from the source to destination), hot (number of hot indicators), num_failed_logins (number of failed login attempts), logged_in (1 if successfully logged in, 0 otherwise), num_compromised (number of compromised conditions), num_file_creations (number of file operations), num_shells (number of shell prompts), num_access_files (number of operations on access control files), is_host_login (1 if the login belongs to the host list, 0 otherwise), is_guest_login (1 if the login is a guest login, 0 otherwise).

3.1.4 U2R Attack

U2R (User to Root) attack in which the attacker starts with access to a normal user account on the system and it can generate some malicious activity to gain root access to the system. Here considering two type of U2R attack detection; buffer_overflow and rootkit. The buffer overflow is a program overwrites the buffer boundary when writing data to a buffer. Rootkit is type of software to hide the presence of certain programs or processes from normal methodswhen it is identified as a malicious program. 8 parameters are using to detect the U2R attack. The parameters are; hot (number of hot indicators), num_compromised (number of compromised conditions), root_shell (1 if root shell is obtained, 0 otherwise), num_root (number of root access), num_file_creations (number of file operations), num_shells (number of shell prompts), num_access_files (number of operations on access control files), is_host_login (1 if the login belongs to the host list, 0 otherwise).

4. ARCHITECTURE OF PROPOSED SYSTEM

4.1 LAYERED APPROACH MODEL

The availability, efficiency, confidentiality and integrity of data ensuring by the Layer based Intrusion Detection System (LIDS). It represents a sequential Layered Approach and services over a network. (Fig 1) The layered model goal is to increase efficiency and reduce computation and the time required to detect anomalous event. Eliminate the communication overhead among different layers in order to reduce the time needed to detect an anomalous event. Make the layers self sufficient to block an attack [10].

An algorithm for intrusion detection system is given below:

Start

Step 1: For each of the test instances performs step 2 through 5.

Step 2: Test each instance and label it either as an attack or normal.

Step 3: If it is named as an attack, block it and go to step 1. Else pass the instance to the next layer.

Step 4: if the current layer is not the last then test the

corresponding instance and go to the above step. Else go to next step.

Step 5: Test the instance and label it as normal or an attack. If it is named as an attack, block it.

End

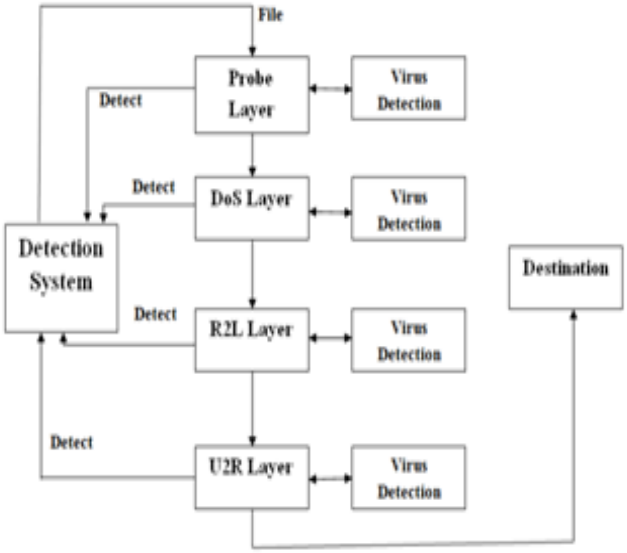

Fig 1: Layered Model for Intrusion Detection

5. EXPERIMENTAL ANALYSIS

The system with randomly selected 1,000 normal records and Probe, DoS, R2L, and U2R records from the training data as the training data for detecting Probe, DoS, R2L, and U2R attacks. The analysis on this proposed approach shows that the layered approach is very effective in restricting the attack traffic to the initial layers and the system is very efficient and accurate.

6. CONCLUSIONS

This system develops an advanced notice board where the registered members can able to post their content and which can be seen by all the users in this world using Android. This system has two types of users; one is admin user and another is member user. The admin user is a super user. Once the member user registers, then they can able to login through their mobile phone and browse the various posting done on the notice board. This system detects 4 types of attack; Probe, DoS, R2L, U2R. It is using Layered Model System for detecting intrusion. It reduces the computation and overall time required to detect the attack and also it improves the speed of the system using pipeline technique.

REFERENCES

[1] SANS Institute—Intrusion Detection FAQ, http://www.sans.org/ resources/idfaq/, 2010.

[2] Y.-S. Wu, B. Foo, Y. Mei, and S. Bagchi, “Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS,” Proc. 19th Ann. Computer Security Applications Conf. (ACSAC ’03), pp. 234-244, 2003.

[3] R. Bace and P. Mell, Intrusion Detection Systems, Computer Security Division, Information Technology Laboratory, Nat’l Inst. of Standards and Technology, 2001.

[4] Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". *Computer Security Resource Center* (National Institute of Standards and Technology) (800–94). Retrieved 1 January 2010.

[5] A strict anomaly detection model for IDS, Phrack 56 0x11, Sasha/Beetle.

[6] Herv´e Debar, An Introduction to Intrusion-Detection Systems.

[7] Mr.C.Saravanan, Mr.M.V.Shivsankar, Prof.P.Tamije Selvy, Mr.S.Anto,
An Optimized Feature Selection for Intrusion Detection using Layered Conditional Random Fields with MAFS, 2012.

[8] Ankita Gaur, Vineet Richariya, A Layered Approach for Intrusion Detection Using Meta-modeling with Classification Techniques.

[9] Brajesh Patel, An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols.

[10] KDD Cup 1999 Intrusion Detection Data, http://kdd.ics.uci.edu/ databases/kddcup99/kddcup99.html, 2010.