RESEARCH ARTICLE OPEN ACCESS

Detection of Network Attacks Using Signature Based Approach

Nikhil Mangrulkar, Arvind. R. Bhagat Patil
Dept. of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur (Maharashtra), India
Email: mangrulkar.nikhil@gmail.com, arbhagatpatil@gmail.com

ABSTRACT
Network attack detection is an essential technology in business as well as dynamic research area. It is essential for information security. Attack on network can cause legitimate users being strived or denied services. A network attack detection approach is designed to detect attacks on network which follows the signature based methodology for ascertaining attacks. This approach maintains a log which shows the list of attacks to administrator for evasive action by generating alerts to control attacks on server.

Keywords - Network attack, signature based attack detection, Denial of Service.

I. Introduction

In computer networks, an attack is an effort to steal, disable, destroy, alter, or obtain unauthorized access to or to make unauthorized use of an asset. Network attacks can cause network services slow, temporarily unavailable, or down for a long period of time. Therefore it is necessary for users and network administrator to detect these attacks before they cause damage to the system. The challenge for the network intrusion detection technology is to achieve real-time under high-speed network intrusion detection.

Denial of Service (DoS) attacks has become a major threat to current computer networks. The aim of a denial of service attack is to oppose authorized users access to a particular resource. Known DoS attacks in the Internet generally conquer the target by exhausting its resources that can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services.

II. Types of Attack Detection Systems

Generally, the behavior of an intruder is noticeably different from that of a legitimate user and hence can be detected [2]. Attack detection systems can be classified based on their deployment in real-time.

A. Host Based Detection

The host based detection systems detects and examines the internals of a computing system rather than its external interfaces [2]. Such systems might detect internal activity such as which program accesses what resources and attempts illegitimate access. An example is a word processor that suddenly and inexplicably starts modifying the system password.

B. Network Based Detection

A network is connected to the rest of the world through the Internet. The Network based detection system reads all incoming packets or flows, trying to find suspicious patterns. For example, if a huge number of TCP connection requests to an extremely large number of different ports are observed within a short time, we could assume that someone is doing a „port scan at some of the computer(s) in the network [2].

III. Proposed Work

A host based attack detection mechanism which focuses on detecting network attacks using signature based methodology is proposed in this paper. Proposed approach checks every packet received at the selected network interface for known attack patterns. A packet is classified as attack packet on detecting improper or missing fields of the received packet. This apporach is used for detecting TCP attack packets and UDP attack packets. For detecting TCP flood attack we have implemented rate limiting Mechanism in which if number of packets received from a particular IP crosses the set threshold value within specified time, packets are classified as TCP flood attack packets.

A. Classifing TCP attack packets.

Among all the packets that have been received on the selected network interface, for classifying an incoming TCP packet as an attacking packet various details of every packet has been checked. For TCP attack traffic following fields are checked-

- Sequence number of the packet – If the sequence number of incoming packet is blank, it is invalid and packet is classified as attack packet.
- Source or destination Port number – If the source or destination port number of incoming packet is invalid (0) then packet is classified as attack packet.
- TCP Header data – If there is no data present in TCP header then such packet is classified as attack packet.
- Checksum – If the packet is having blank checksum value then it is classified as attacking packet.
- Flags – If all the flags of received TCP packet are set to zero then packet is classified as attack packet.

B. Classifing TCP SYN Flood attack packets.

For classifying incoming packets as SYN Flood packets, rate limiting technique has been used. If number of packets that have being received from a particular IP and Port number with its SYN flag set, crosses the set threshold value that has been set, then those packets are classified as SYN flood attack packets.

C. Classifing UDP attack packets.

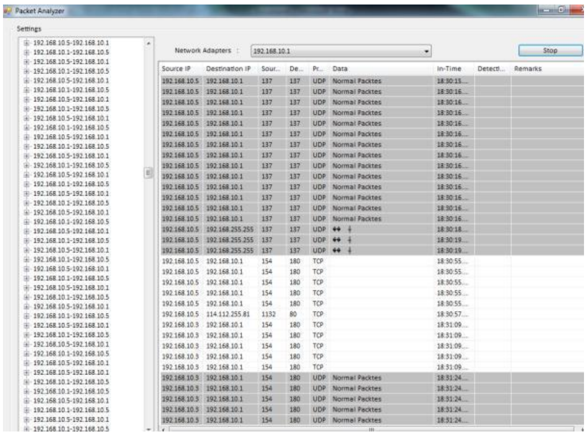
For classifying an incoming UDP packet as an attack packet various details of every packet has been checked. For UDP attack traffic following fields are checked-

- Source or destination Port number – If the source or destination port number of incoming packet is invalid (0) then packet is classified as attack packet.
- Checksum – If the packet is having blank checksum value then it is classified as attacking packet.
- Length – If the length of packet field of the received packet is 0 or blank, then it is classified as attack packet.

to take evasive actions to prevent DoS attacks on the network. With further modifications, this approach can also be used for detecting DDoS attacks on the network.

IV. Implementation

For packet capturing and checking various fields of packets detection approach is developed using Microsoft® Visual Studio®. Fig. 1, shows user interface on which details of every packet that has been received on the selected network interface is displayed. Details include: Source IP and Source port of the packet, Destination IP and Destination port, Type of packet (TCP / UDP), Data, In-time of packet and the time at which that packet was classified as attack packet, Remarks which specifies type of attack that has been classified by the approach.



192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5
192.168.10.5-192.168.10.1
192.168.10.1-192.168.10.5

Network Adapters : 192.168.10.1

Source IP	Destination IP	Sour...	De...	Pr...	Data	In-Time	Detecti...	Remarks
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:15...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.10.1	137	137	UDP	Normal Packtes	18:30:16...		
192.168.10.5	192.168.255.255	137	137	UDP	◆◆ ǂ	18:30:18...		
192.168.10.5	192.168.255.255	137	137	UDP	◆◆ ǂ	18:30:19...		
192.168.10.5	192.168.255.255	137	137	UDP	◆◆ ǂ	18:30:19...		
192.168.10.5	192.168.10.1	154	180	TCP		18:30:55...		
192.168.10.5	192.168.10.1	154	180	TCP		18:30:55...		
192.168.10.5	192.168.10.1	154	180	TCP		18:30:55...		
192.168.10.5	192.168.10.1	154	180	TCP		18:30:55...		
192.168.10.5	192.168.10.1	154	180	TCP		18:30:55...		
192.168.10.5	114.112.255.81	1132	80	TCP		18:30:57...		
192.168.10.3	192.168.10.1	154	180	TCP		18:31:09...		
192.168.10.3	192.168.10.1	154	180	TCP		18:31:09...		
192.168.10.3	192.168.10.1	154	180	TCP		18:31:09...		
192.168.10.3	192.168.10.1	154	180	TCP		18:31:09...		
192.168.10.3	192.168.10.1	154	180	TCP		18:31:09...		
192.168.10.3	192.168.10.1	154	180	UDP	Normal Packtes	18:31:24...		
192.168.10.3	192.168.10.1	154	180	UDP	Normal Packtes	18:31:24...		
192.168.10.3	192.168.10.1	154	180	UDP	Normal Packtes	18:31:24...		
192.168.10.3	192.168.10.1	154	180	UDP	Normal Packtes	18:31:24...		
192.168.10.3	192.168.10.1	154	180	UDP	Normal Packtes	18:31:24...		

Fig 1. User interface

Fig. 2, shows the display of detection of TCP and UDP attacks that were initiated simultaneously. UDP attack packets are highlighted in Brown color whereas TCP attack packets are highlighted in Red color. Normal TCP packets are displayed in White background while normal UPD packets are displayed with Silver background.

ig. 3, shows simultaneous detection of TCP flood attack packets, TCP attack packets and UDP attack packets. Packet at which incoming TCP packets are classified as Flood attack packets is highlighted in Orange color.

REFERENCES

[1] N. Wattanapongsakor n, S. Srakaew, E. bat, C. Sribavonmongkol, T. Junhom, P. Jongsubsook, C. Charnsripinyo, "A Practical Network-based Intrusion Detection and Prevention System", *11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2012.

[2] Monowar H. Bhuyan, D. K. Bhattacharyya and J.k Kalita, "Network Anomaly Detection:Methods, Systems and Tools", *IEEE Communications Surveys & Tutorials*, 2013.

[3] Zhiyuan Tan, Aruna Jamdagni, Xiangjian

He, Priyadarsi Nanda and Ren Ping Liu, “Triangle-Area-Based Multivariate Correlation Analysis for Effective Denial-of-Service Attack Detection”, *11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2012.

[4] A. Kumaravel, M. Niraisha, “Multi-Classification Approach for Detecting Network Attacks”, *IEEE Conference on Information and Communication Technologies*, 2013.

[5] Risto Vaarandi, “Detecting Anomalous Network Traffic in Organizational Private Networks”, *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, San Diego, 2013.

[6] Shin-Ying Huang, Yen-Nun Huang, “Network traffic anomaly detection based on growing hierarchical SOM”, *43rd IEEE/IFIP Annual International Conference on Dependable Systems and Networks*, 2013

[7] B.S. Kiruthika Devi, G. Preetha, S. Mercy Shalinie, “DDoS Detection using Host-Network based Metrics and Mitigation in Experimental Testbed”, *International Conference Recent Trends In Information Technology*, 2012.

[8] Y. Xie, S. Tang, X. Huang, C. Tang, X. Liu, “Detecting latent attack behavior from aggregated Web traffic”, *International Journal on Computer Communications, Vol 36, Pg. 895– 907,* 2013.

[9] P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, “Network Intrusion Detection with Fuzzy Genetic Algorithm for Unknown Attacks”, *IEEE International Conference on Information Networking*, 2013.

[10] Ahmad Sanmorino, Setiadi Yazid, “DDoS Attack Detection Method and Mitigation Using Pattern of the Flow”, *IEEE International Conference of Information and Communication Technology*, 2013.

[11] Sumaiya Thaseen, Ch. Aswani Kumar, “An Analysis of Supervised Tree Based Classifiers for Intrusion Detection System”, *IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering*, 2013.

[12] Kapil Wankhade, Sadia Patka, Ravinrda Thool, “An Overview of Intrusion Detection Based on Data Mining Techniques”, *IEEE International Conference on Communication Systems and Network Technologies*, 2013.