ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Behavioral –based feature selection approach in NIDS

Amruta S. Solanke [1], Nitin R. Chopde[2], Manjiri U. Karande[3]

P.G. Student, Department of Computer Engineering, Padm. Dr. V. B. Kolte COE, Malkapur, Maharashtra, India[1]

Assistant Professor, Department of Computer Science Engineering, G. H. Raisoni COEM, Amravati, Maharashtra, India[2]

Assistant Professor, Department of Computer Science Engineering, Padm. Dr. V. B. Kolte COE, Malkapur, Maharashtra, India[3]

ABSTRACT:Now days it isessential to preserve a high level security to ensure secure and trusted communication of information between different organizations. Intrusion Detection System is a novel safeguard technology for systemsecurity after conventional technologies, such as firewall, message encryption and so on.The end-user machines are desired to defend by the Network Intrusion Detection System (NIDS) from threats. An efficient NIDS is consequently a network security system proficient of protecting the end user machines well before a threat or intruder affects. NIDS necessitate a space proficient data base for detection of threats in high speed environment. A bloom filter is a space proficient randomized data structure intended for representing a set in order to hold up membership queries.In this, a proposed system NIDS located at the network egress points to detect malware infections inside the networkcombined with DNS traffic analysis.The experimental result shows that this security approach is sufficient for improving the sustainability of the system and is good at detectingmalware infections.

KEYWORDS:Intrusion Detection System, NIDS, Bloom filter.

I. INTRODUCTION

At this time the number of computer networks keeps rising in correspondingthrough transactions, especially on the Internet while streaming, video conferencing, chatting, searching, etc. These different types of transactions commence many intrusions and anomalies into the network. Network traffic is frequently seen to display abrupt deviations from normal behaviour. By malicious network attacks such as Denial-Of-Service or viruses a few of these aberrations are caused, while others are the result of equipment failures and accidental outages [1]. Many methods have been developed by organizations and play very imperative roles to secure network infrastructure and connections via the Internet viaall over the use of firewalls, anti-virus software packages and intrusion detection systems. Recent firewalls cannot protect against eachtype of intrusion, whereby several intrusions obtain advantages of computer system vulnerabilities [2]. An intrusion detection system (IDS) provides in the region of the clock network observation and is an additional wall to secure the network. The intrusion detection system is a process of determining an intrusion into a system throughout the observation of accessible information connecting to the state of the system, monitoring user activities and reporting to a management station [3]. Consequently, the Intrusion Detection techniques are classified into host-based and network-based depending on the type as well as source of information used to recognize security violate [4, 5] depending on the technique of intrusion detection. One definition from the study that an intrusion is any activity that moves a system from a secure state to an insecure state, except this does modest to clarify the situation. There is one more definition that declares in essence, an intrusion is anything that violates the policy of a site under deliberation, but this also does little to address the issues at hand.Nowhere each word of intrusion detection (ID) is defined as, Intrusion: The act of wrongfully entering upon, seizing, or taking possession of the property of another.Detection: The act of discovering or determining the existence, presence, or fact of. Intrusion Detection: The

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

act of discovering or determining the existence, presence, or fact of the wrongfully entering upon, seizing, or taking possession of the property of another.
The intrusion detection system and the conception of security might be threatening and complex. To develop a tool that arbitrate the user and the operations to achieve security goals is the objective of the paper. Theresultant product will have the following belongingsas a platform independent tool with user-friendly graphical user interface, using previously existing techniques and notion for intrusion detection system. Citizenshave touse the intrusion detection system in order to recognize attacks in host based system and network based system. The operations include bunch of rules to identify the attacks of foreigners to reach and read private files that is placed in personal computer or the owner would like to send anywhere. Computers directlylinked to the Internet are focus to persistent probing and attack. While protective actions such as secure configuration, up to date patching, and firewalls are all prudent steps, they are intricate to maintain and cannot guarantees that all vulnerabilities are defended. IDS providedefence in profundity by detecting and logging aggressive activities. An IDS system acts as eyes that observe for intrusions when other protective actions fail, tested.

II. RELATED WORK

Observing network resources,detecting anomalous behavior andexploitation in network are the objectives of intrusion detection system[6]. Intrusion detection perception was introduced in early 1980's after theevolution of internet with scrutiny end monitoring the threat [7]. There was anabruptincrease inreputation and amalgamation in security infrastructure.James Anderson's wrote apaper for a government organization and imported a move in the direction of that audit trails containedsignificant information that could be expensive in tracking exploitation and understanding of userbehavior [6].
OpenSec isan OpenFlowbased network securityframework through the intention of allowance to campus operators forapplying securitypoliciescrossways the network. This work is motivated by taking into accounta campus operator needs to reflect incoming web traffic toan intrusion detection system (IDS) and e-mail traffic to aspyware detection device. Our goal is to leverage SDN to allowthe operator to write a high-level policy to achieve this, insteadof having to manually configure each device.Additionally,suppose the IDS getdetected malicious traffic and a sender wantsto be blocked from accessing the network. Instead of havingthe operator, the edge router is configuring to manually disableaccess to the source; they are interested in blocking the senderautomatically [8].
To generate rules for IDS, Lee et al. proposed a system using mutual misuse and anomaly detection approaches [9]. Multiple model cost based approaches are applied for improving efficiency. These evaluate and identify models with high accuracy but low cost. A dispersed architecture is proposed for evaluating models in real time. To develop usability adaptive learning algorithms are used for incremental updates. To decrease reliance on the labeled data unsubstantiated learning is studied.
To detect various types of attacks like TCP SYN Flood, Back/Land, and Buffer over Flow and Abnormal packets a hybrid IDS system is used in N/W IDS and for Host IDS UN-authorize accessing and login/logout failed. The system is providing both type of functionality in one system which is improving overall efficiency of the existing IDS [10].
A bloom filter is aneasy, space-efficient, randomized data structure for succinctly a static data set also great potential for scattered applications where systems need to share information about what resources they have. At the cost of a small probability of false positive membership queries the space efficiency is achieved[11].

III. PROPOSED WORK

The virus attacks are expanding on the web these days. It is a constant or persistent hacking process and set of stealthy focusing on a particular entity with high-value information, for example, government, military and the monetary business. An intend of a virus or malware is to steal the information or to make damage the association or system. Just the once installing hence as to hack into the system has been accomplished, malware on the contaminated machine by attacker. For instance, malware is, Trojan horse or backdoor secondary passage, is customized for firewalls and anti-virus software of the target network. A system is not merely utilized for remotely controlling the traded off machine in the malware or attack, but also to steal touchy information from extended period of time. The proposed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

system Behavioral-based feature selection approach in NIDSwhich is a virus detection system placed at the network egress points to detect malware infection.

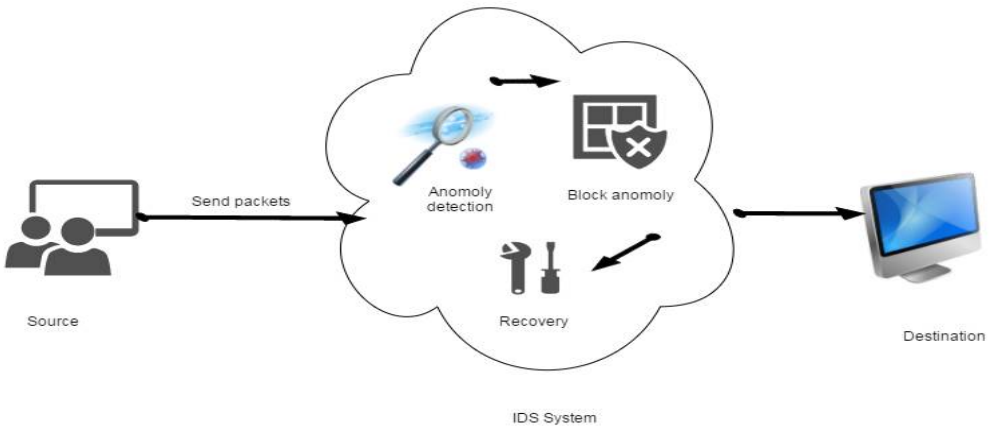

Fig. 1: Architecture of NIDS

It will works as the sender PC sends the single or multiple files to destination PC,implementing intrusion detection system in between sender and destination which is placed at destination side like a firewall or antivirus.The IDS will first detect the malicious anomalies in the file sending from the sender side with help of malicious anomaly list provided by database.
The IDS will recover the affected file if any by using bloom filter mechanism by creating the replica of that victim file which is the main task performed by IDS after detecting the malicious file to reduce the error bit rate i.e. to avoid the data thrashing.The destination side will receive the files which are malicious free and get acknowledged by IDS about malicious attack.

- **AES Algorithm**

A set of specially derived keys called round keys are used in encryption process. These are applied, along with additional operations, on an array of data that holds exactly one block of data. This array we called as the state array.
So let's consider the following AES steps of encryption for a 128-bit block:

- First derive the set of round keys from the cipher key.
- Then, initialize the state array with the block data (plaintext).
- After that, add the initial round key to the starting state array.
- Then, perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- At last, copy the last state array out as the encrypted data (cipher text).

The motive that the rounds have been listed as- "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

- **Bloom Filter**

A bloom filter is aneasy, space-efficient, randomized data structure for succinctly a static data set, huge potential for scattered applications where systems need to share information about what resources they have. The space efficiency is achieved at the cost of a small probability of false positive membership queries.
In the NIDS the bloom filter implementing a mechanism to decrease the error bit rate of proposed system, the bloom filter will detect the malicious content file and also the file which has been affected the normal file so that to block the malicious file and to recover the affected file by creating a proxy or replica of that victim file.
At the heart of every bloom filter lays two key elements
1. Consider an array ofn bits, initially all bits are set to 0.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

2. A group of k independent hash functions h(x). Every hash function takes a value and generate a number i, where i < n which efficiently maps to a position in a bit array.

➢ **Operation**

Input:

A=array of anomalies // malicious anomaly list
S= array of signature // malicious signature list
FN= input file to be checked
FM= Malicious files list // used to infect the normal file

Output:

1. Malicious anomaly in the file
2. List out the signature attached to file
3. File attack to show file infected
4. Recovery of infected file in the form of creating copy or proxy dynamically

Process:

Step 1: read the input file FN
for j = 0 to n do //every string in FN where n denotes the reading file up to end line by line
check = FN[j] // taking each string to check variable
i = 0
4: while i <A. lengthdo
if check equals A[i] Then
FN is has malicious anomaly
get signature of FN
k=0
sign = FN.sign
while k<S. length do
if sign equals S.[k] then
FN has malicious signature
Else
Add sign to S
end of while
end if
end while
end for
end

IV. EXPERIMENTAL RESULTS

The following Table-1 shows the effective experimental result of the proposed system comparing to the existing system considering the parameters Anomaly Detection, Signature Detection, Recovery, Accuracy and Time.

Parameters	Existing (%)	Proposed(%)
Anomaly Detection	80	90
Signature Detection	60	100
Recovery	40	90
Accuracy	70	100
Time	90	50

Table-1: Experimental Result

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

The Fig. 2 shows the graph comparison considering the parameters Anomaly Detection, Signature Detection, Recovery, Accuracy and Time in between proposed system and existing system.

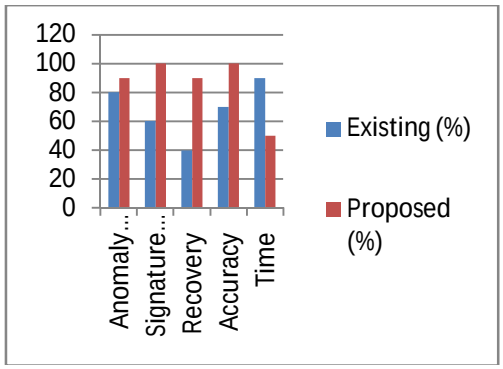

Fig. 2: Result analysis

V. CONCLUSION

In this paper, a proposed system NIDS placed at the network egress points to detect malware infections inside the networkcombined with DNS traffic analysis. The experimental results show that this security approach is feasible for improving the sustainability of the system and is good at detecting malware infections. It is a useful network intrusion detection system that can assist to fight against cyber-crime such as theft of information from infected host.

REFERENCES

[1] Chundong Wang, Quancai Deng, Qing Chang,Hua Zhang and Huaibin Wang " A New Intrusion Detection System Based on Protocol Acknowledgement", 2010 International Conference on Multimedia Technology, IEEE, pp.1-4, Oct. 2010.
[2] Jin-Tae Oh , Sang-Kil Park, Jong-Soo Jang and Yong-Hee Jeon "Detection of DDoS and IDS Evasion Attacks in a High-Speed Networks Environment", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.6, pp.124-131, June 2007.
[3] Vera Marinova-Boncheva "A Short Survey of Intrusion Detection Systems", pp.23-30, 2007
[4] Moad Alhamaty , Ali Yazdian and Fathi Al-qadasi "Intrusion Detection System Based On The Integrity of TCP Packet", World Academy of Science, Engineering and Technology, Vol.1, No.11, pp.3720-3724, Nov. 2007.
[5] T. S. Sobh "Wired and wireless intrusion detection system Classifications, good characteristics and state-of-the-art", Computer Standards & Interfaces, Vol. 28, Issue 6, pp. 670-694, Sept. 2006.
[6] Asmaa Shaker Ashoor, Prof. Sharad Gore – "Importance of Intrusion Detection System", International Journal of Scientific& Engineering Research, Vol. 2, Issue 1, Jan. 2011.
[7] Paul Innella- "The Evolution of Intrusion Detection Systems", Tetrad Digital Integrity, LLC. International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.4, No.1, Feb. 2015
[8] A. Lara and B. Ramamurthy, "OpenSec: Policy-Based Security Using Software-Defined Networking", IEEE Transactions on Network and Service Management, Vol.13, Issue 1, pp. 30-42, March2016.
[9] Wenke Lee and S. J. Stolfo, P. K. Chan, E. Eskin, Wei Fan, M. Miller, S. Hershkop and JunxinZhang" Real Time Data Mining-based Intrusion Detection", DARPA Information Survivability Conference ; Exposition II, 2001. DISCEX '01. Proceedings, IEEE, Vol. 1, pp. 89-100, IEEE, June 2001.
[10] Kiran Dhangar, Deepak Kulhare, Arif Khan, "A Proposed Intrusion Detection System", International Journal of Computer Applications (0975 – 8887) Vol. 65, No.23, pp.46-50, March 2013.
[11] Deke Guo, Jie Wu, Honghui Chen, and XueshanLuo, "Theory and Network Applications of Dynamic Bloom Filters", Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, IEEE, pp.1-12, April 2006