IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

A Real Time Approach to Strengthen Computer Security By Host Cum Network Agent Based Intrusion Detection System (HCN-AIDS)

S. K. Tiwari[1]*, D. S. Pandey[2], V. Namdeo[3]

[1] Information Technology, RKDF-Institute of Science & Technology, RGPV, Bhopal, India
[2] Information Technology, RKDF-Institute of Science & Technology, RGPV, Bhopal, India
[3]Computer Science/ Information Technology, RKDF-Institute of Science & Technology, RGPV, Bhopal, India

Corresponding Author:shivendrakt2018@gmail.com

Available online at: www.ijcseonline.org

Accepted: 18/July/2018, Published: 31/July/2018

Abstract- To enhance and strengthen the security features of computer`s information. As for as term Computer security is concern; it is the process of collecting information about unauthorized access. Detection is a recognition process which helps us to determine if someone tried to enter the target system successfully or not. Although there are so many methodologies has been also developed to make secure the secret and private information but still there is occurrence of unauthorized access of information takes place and violate the existing meaning, features and functionalities. Such unauthorized users are called as Intruders. These are also called as attackers or crackers. An attacker may not care about our identity and their action effects often try to take control of the computer to launch attacks on the computer systems secretly. In this research work it is focused to develop such a strong intrusion detection system which can silently and efficiently capture the intrusions penetrating in individual host systems or any host of the network system dynamically. This is "A Real Time Approach to Strengthen Computer Security by Host cum Network Agent Based Intrusion Detection System (HCN-AIDS)"which will enhance efficiency as compared to earlier agent based intrusion detection system. It includes powerful agents equipped with strong unique functionalities like Network Agent, Mobile Agent, Intrusion Detection Agent, Rule agent etc. this research model is again becomes more important and useful because works in hybrid mode i.e. in real time data as well host based systems and generates efficient results.

Keywords- Attacks, Crackers, Information, Detection, feature, Host, Intruder, Intrusion, Mobile Agent, Network Agent, security etc.

I. INTRODUCTION

To prevent and detect the unauthorized access of any computer is a concern of Computer security [1]. Intruders with the help of some means of communication take over advantages of computers various things in the way of banking and investing to shopping [1]. Usually attackers get control on target systems like government or financial firms systems, this will provide them an ability to make hidden them as well as their actual locations and hence intrusions/ attacks easily can be launched [2].

The difficulty in software makes it difficult high to thoroughly test the security of computer systems. Although, it`s up to the user, to obtain and install file patches, perform the configuration of the software for operating in more secure manner [3]. There are some more risks which could be faced even if users weren't connected to the Internet like hard disk failures, theft, power outages, etc. The bad news caused by this problem is that it possibly unable to plan for all possible risks [4].

I.I Intrusion

Table 1 depicts types of attacks that occur in network. Frequently, intrusions are caused by an outside attacker accessing the system from the Internet or local network or the operating system of the infected machine or uses the security flaw of a third-party application (middleware), or by inside attackers who may be authorized users in some respects attempting to gain and misuse non-authorized security and system privileges [1-7].

I.II IDS Obstacles

There are following basic issues; in the IDS functioning identified [5-9].

- Breadth of Attacks:
- Burdensome Maintenance
- End-to-end Encryption
- Flexibility
- High Speed Communications
- Large False Positives

Intrusion Detection & Prevention

To identify the attacks in individual host system and network system functional system capture and analyze the packets and maintain the logs as for example host logs given below:

- Application logs
- Device-related logs
- Kernel logs

There are some issues observed below in both kinds of IDSs whether it is HIDS or NIDS [8]:

- Additional activities for security such as logging.
- Difficulty in recognizing network-wide attacks.
- Heterogeneous operating systems.
- Insufficient computational capability to deploy complete host-based IDS.
- Increased number of critical nodes in the network. [10].

The act of avoiding detected harmful suspected data set in real-time by not allowing it to execute or continue to its destination is termed as Prevention of Intrusion. It is useful against denial of service, floods, brute force attacks, vulnerability detection, protocols anomaly detection and prevention against unknown exploits within the host as well as network based systems [10-15]**.**

The aim of this paper is to recommend architecture for the intrusion detection systems that can adapt to the future threats with the help of various types of agent interactions. The other part of this paper includes four more sections like section II related research work studies whereas section III states all about this newly proposed model its concept architecture, algorithm and working phases. Finally section IV comprises with results data and its analysis and section V concludes its impact use and future scope.

Table 1: Layer wise Attacks

S. No.	TCP/IP Layer	Attacks	Attacks Type
1	Application Layer	▪ DoS ▪ U2R ▪ R2L	▪ Back ▪ Land ▪ Buffer-overflow ▪ FTP-Write ▪ Portsweep ▪ Nmap
2	Transport Layer	▪ DoS ▪ R2L	▪ Land ▪ Multihop

II. RELATED WORK

[1] A.M. Riyad, M.S. Irfan Ahmed and R.L. Raheemaa Khan "Multi agent based intrusion detection architecture for the IDS adaptation over time", addresses a problem that current intrusion detection systems suffer. Intrusion detection systems highly rely on the previous patterns of attacks as well as the deviations of the normal patterns. This will lead to inefficiency as novel attacks can occur in the future due to the ever changing network and hosts configurations and technologies.

[2] Mohiyeddin Mozaffari and Behrouz Safarinejadian,"Mobile-agent-based distributed variational Bayesian algorithm for density estimation in sensor networks" considers the problem of probability density estimation and model order selection in distributed sensor networks.

[3] Chaimae Saadi ,Ensak-Morroco and Habiba Chaoui "Intrusion detection system based interaction on mobile agents and clust-density algorithm "IDS-AM-Clust" this work falls within the framework of the new generation of intrusion detection systems able to detect known and unknown attacks and reduce the rate of false positives and negatives, by coupling two recent technologies: mobile agents and a new data mining algorithm Clust-density in one single IDS named IDS-AM-Clust.

[4] Sara Chadli,Mohamed Emharraf and Mohammed Saber "The design of an IDS architecture for MANET based on multi-agent" this architecture is a combination model hierarchical based on clusters and cooperation model based on a multi-agent system (SMA). In this architecture, agents use knowledge related to global security ontology, it can be used to infer new detection rules.

[5] Okan Can "Mobile agent based intrusion detection system" aimed to combine IDS with Mobile Agent concept for more scale, effective, knowledgeable system.

[6]Wang Yu, Cheng, Xiaohui and Wang Sheng "Anomaly Network Detection Model Based on Mobile Agent" includes important usage of mobile agents for efficient intrusion detection.

III. PROPOSED WORK

In this proposed model it is tried to conceptualize that this intrusion detection system will fulfill detection functionality simultaneously in host mode and network mode. For the same purpose it includes various agents to serve their corresponding functionalities. The proposed model has designed for Agent based intrusion detection system and evaluates behavior of normal and abnormal data packets. In this research will provide a better Agent based intrusion

detection model which will be work either on real time data packet or KDD'99 data set to fulfill requirement of network security. The performance of the proposed model will evaluate by measuring the average normal and abnormal behavior of data packets, which also compared with the average execution time for a number of currently use network security techniques. Host cum Network Agent Based Intrusion Detection System monitors each system in the network. In this case, the agents of the IDS are located inside of the host to monitor system behavior [13]. Host-based IDSs can be quite effective in switched environments, whereas network-based IDS systems are less effective in that environment. A switch tends to isolate communications on the network, making it difficult for network-based IDS to monitor all traffic. However, if the systems on the switched network have host-based IDSs installed, potential attacks may be thwarted [16-17].

In this model data packet will analyze through network admin for network data and host admin for local machine data. Initially it will prepare training data set then start capture data from network as well as local machine to find intrusion. There are following basic agents prepared in this model as given below

- AA: Alarming Agent
- IDA: Intrusion Detection Agent
- MA: Mobile Agent
- NA: Network Agent/Host Agent
- SA: Signal Agent
- TA: Tenet Agent

III.I Proposed IDS Architecture

Architecture of Proposed Intrusion Detection is shown in Figure-1: A real Time Host cum Network Agent based Intrusion detection System (HCN-AIDS). In this six agents based system all agent works together but they do not acquire the data from the network/host directly, but receive/capture the preprocessed data in proper way.

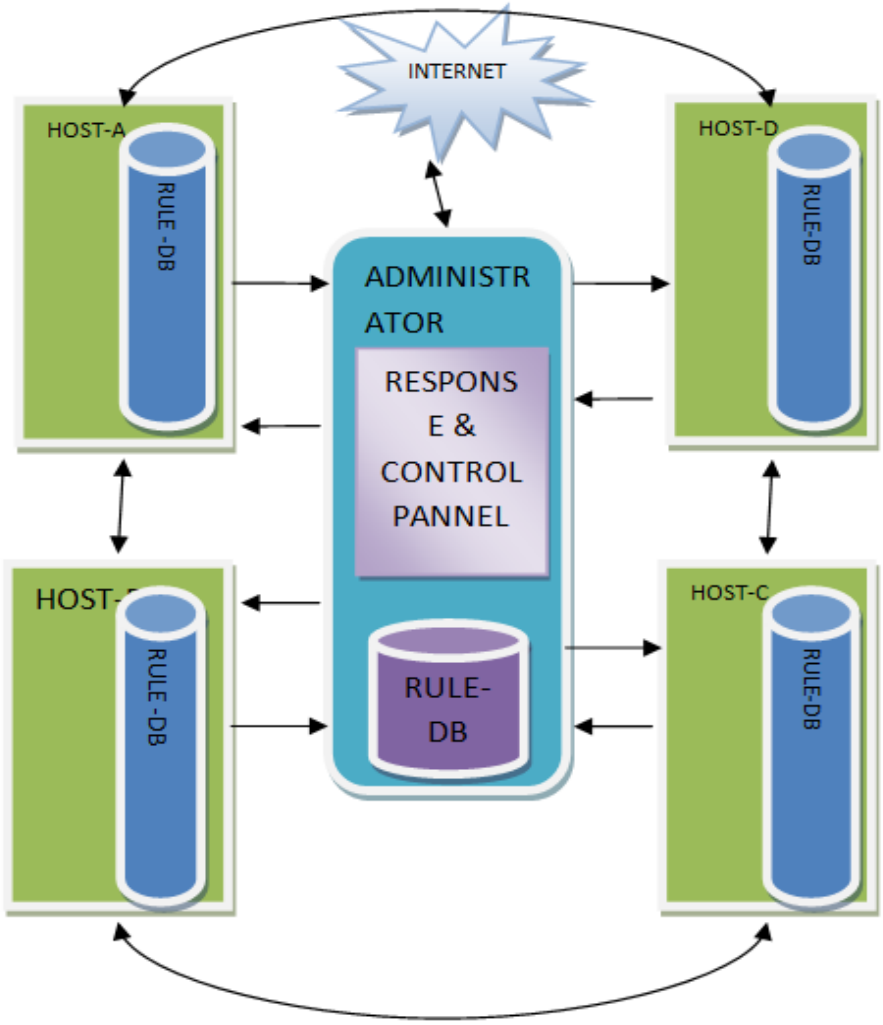


Figure 1: A Real Time Proposed Host cum Network Agent Based Intrusion Detection System (HCN-AIDS) Architecture

III.II Proposed Technique

The introduced model here works in binary mode simultaneously and individually as well.

Network Mode:

In this mode proposed system works in following steps:

Step 1: Activates all connected nodes of network by Mobile Agent.

Step 2: With the help of Network Agent starts capturing packets and extracting their features.

Step 3: With the help of rule database by Rule Agents packet features measured and identified by Intrusion Detection Agent

Step 4: Finally Alarm Agent generates alarm to affected node.

Host Mode:

If Cap_ Value > TH

Then

Intrusion Detection Agent Activate

Else

Intrusion Detection Agent Deactivate

Rule Agent Calculated tenet

Authentication_Recorded_Value→

User_Auth = Wrong(Password) > Match(M)

Where M is 3 time

Working_Time_Recorded_Value→

Time = Log_In→10 AM

&

Log_Out→5 PM

III.III Proposed Algorithm

If (Node is in the network)

NAs();

attack_result =Rule_db();

Else

attack_result =Rule_db();}}

Response _Node-i(){

If (attack_result==0)

Packet_cap(),

Else

AA();}}

MAs(){

i. Send Mobile Agents to all hosts

ii. Activate hosts

}

NAs(){

i. Activate packet receiving ports

ii. Identify packet type

iii. Identify packet layer

}

Rule_db(){

If local credential== True;

Then Check

If(

IF (Cap_Pack.Flag-> “SF”==0)

IF (Dst_Host_Ser_error_Rate<0 to 1>)

IF (Dst_Host_Ser_Rerror_Rate<0 to 1>)

IF (Dst_Host_Ser_Serror_Rate<0 to 1>)

IF (Dst_Host_Server_Rate<0 to 1>)

IF (Dst_Host_Ser_Diff_Host_Rate<0 to .44>)

IF (Dst_Host_Same_Src_Port_Rate<0 to 1>)

IF (Dst_Host_Diff_Ser_Rate<0 to 1>)

)

Return (DOS);

Else if(

IF (Cap_Pack.Flag-> “RSTO” || “REJ” || “SF”)

IF (Dst_Host_Ser_error_Rate< 0 to 1 >)

IF (Dst_Host_Ser_Rerror_Rate< 0 to 1 >)

IF (Dst_Host_Ser_Serror_Rate< 0 >)

IF (Dst_Host_Server_Rate< 0 >)

IF (Dst_Host_Ser_Diff_Host_Rate< 0 to 1>)

IF (Dst_Host_Same_Src_Port_Rate< .01 to 1>)

IF (Dst_Host_Diff_Ser_Rate< 0 || 1 >)**)**

Return (Probe);

Else if(

IF (Cap_Pack.Flag-> "SF")

IF (Dst_Host_Ser_error_Rate< 0 >)

IF (Dst_Host_Ser_Rerror_Rate< 0 >)

IF (Dst_Host_Ser_Serror_Rate< 0 >)

IF (Dst_Host_Server_Rate< 0 >)

IF (Dst_Host_Ser_Diff_Host_Rate< 0 to 1>)

IF (Dst_Host_Same_Src_Port_Rate< .5 to 1>)

IF (Dst_Host_Diff_Ser_Rate< 0 >)**)**

Return (R2L);

Else if(

IF (Cap_Pack.Flag-> "SF" || "S3" || "RSTR" || "RSTO")

IF (Dst_Host_Ser_error_Rate< 0 to .96 >)

IF (Dst_Host_Ser_Rerror_Rate< 0 to .96 >)

IF (Dst_Host_Ser_Serror_Rate< 0 to 1 >)

IF (Dst_Host_Server_Rate< 0 >)

IF (Dst_Host_Ser_Diff_Host_Rate< 0 || 1>)

IF (Dst_Host_Same_Src_Port_Rate< .02 to 1>)

IF (Dst_Host_Diff_Ser_Rate< 0 >)

Return (U2R)

Else

Return (0);

}

AA(){

i. Send alarm message to client

ii. Abandon the source layer

}}

Stop.

IV. RESULTS ANALYSIS

By this model I have observed the capturing of many kinds of attacks in encountered indifferent layers of TCP/IP like R2L, Probe, DoS and U2R. These results are collected by keen observation of this proposed model in with firewall configuration as well as without firewall configuration. It also includes intrusion detection feature for host as well as network system simultaneously. One thing which makes more valuable to this working model is its real time functioning on live network data which is being mentioned as an example result of observation of 5 days. Configuration of the implementation machine is Pentium Dual Core J2900 2.41 GHz, 4 GB RAM, in which routine data is accumulating and viewing. Result observations are given in Table2 for Host mode and for Network Mode in Table 3 with enabled security Firewall and Table 4without security concern disabled firewall.

Table 2: Host mode observation

S. No.	L_ID	L_PW	Date	Time	Status
1	Abc	Abc	07/06/18	06:10:33	Wrong Time
2	Pqr	Pqr	08/06/18	07:55:58	Wrong Time
3	Abc	Abc	09/06/18	05:02:34	Wrong Time
4	Lmn	Lmn	10/06/18	06:04:12	Wrong Time
5	Efg	Efg	11/06/18	05:30:34	Wrong Time

Table 3: Network mode observation with firewall enabled

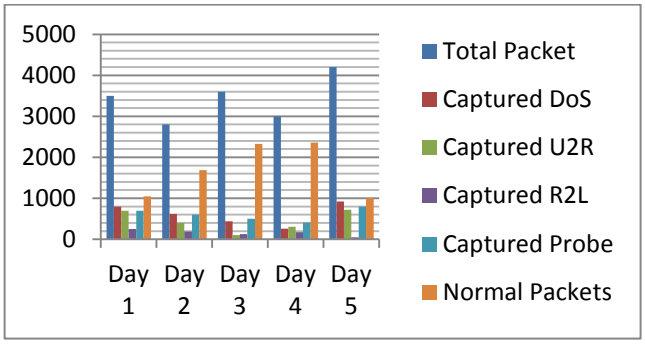
Days	Total Packet	Captured DoS	Captured U2R	Captured R2L	Captured Probe
Day 1	300	25	10	12	18
Day 2	200	22	14	21	19
Day 3	320	32	10	19	24
Day 4	290	41	32	45	12
Day 5	380	23	29	39	16

Table 4: Network mode observation without firewall enabled

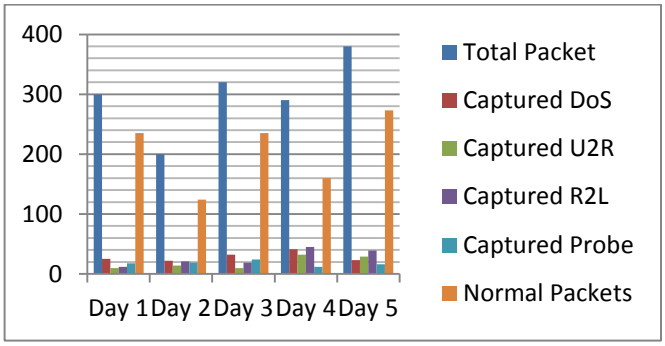
Days	Total Packet	Captured DoS	Captured U2R	Captured R2L	Captured Probe
Day 1	3500	800	700	250	700
Day 2	2800	620	400	190	602
Day 3	3600	440	100	130	504
Day 4	3000	260	305	170	406
Day 5	4200	922	720	52	800

Here graphical representation in Graph for various modes of intrusion detection given below in which Graph 1 represents Attack analysis without firewall in Network mode and Graph 2 denotes the Attack analysis with firewall in Network mode.

Graph 1: Attack analysis without firewall in Network mode

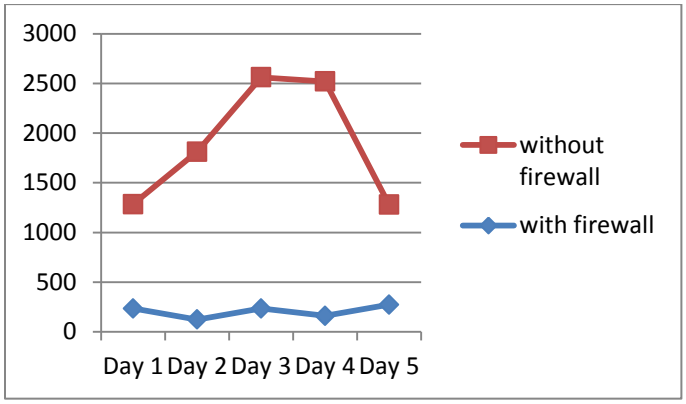


Graph 2: Attack analysis with firewall in Network mode



After observing above statistics in different functional modes it is further need to analyze number of normal packets captured which can been seen in Graph 3 representation as below:

Graph 3: Comparison of normal captured packets



V. CONCLUSION

With the help of this real Time Host cum Network Agent based Intrusion detection System (HCN-AIDS) intrusion capturing becomes easier and efficient because here use of mobile agent, detection and rule agent includes high performance efficiency. This research work is also better in terms of finding source layer of attacks with the extraction packet features.

Some features can be further added in this like to identify intrusions by artificial intelligence algorithm on the basis of learning methods and may include strong prevention mechanisms.

REFERENCES

[1] A.M. Riyad, M.S. Irfan Ahmed and R.L. Raheemaa Khan "Multi agent based intrusion detection architecture for the IDS adaptation over time", Second International Conference on Electrical, Computer and Communication Technologies (ICECCT),IEEE,2017

[2] Mohiyeddin Mozaffari and Behrouz Safarinejadian,"Mobile-agent-based distributed variational Bayesian algorithm for density estimation in sensor networks" IET Science, Measurement & Technology Volume: 11, 2017

[3] Chaimae Saadi ,Ensak-Morroco and Habiba Chaoui "Intrusion detection system based interaction on mobile agents and clust-density algorithm "IDS-AM-Clust", International Colloquium on Information Science and Technology (CiSt),IEEE,2016

[4] Sara Chadli,Mohamed Emharraf and Mohammed Saber "The design of an IDS architecture for MANET based on multi-agent" International Colloquium on Information Science and Technology (CiSt),IEEE,2014

[5] Okan Can "Mobile agent based intrusion detection system", 22nd Signal Processing and Communications Applications Conference (SIU), 2014

[6]Wang Yu, Cheng, Xiaohui and Wang Sheng ,"Anomaly Network Detection Model Based on Mobile Agent", IEEE,Third International Conference on Measuring Technology and Mechatronics Automation, 2011

[7] Ionita, I.; Ionita, L. "An agent-based approach for building an intrusion detection system" Published in Networking in Education and Research, 2013 RoEduNet International Conference 12th Edition, 2013

[8] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma "AgentOuro: A Novelty Based Intrusion Detection and Prevention System" Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on 3-5 Nov. 2012

[9] Vasima Khan, Anomaly Based Intrusion Detection And Prevention System, IJERT, 2013

[10] Mukesh Sharma,Akhil Kaushik, Amit Sangwan Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort.,IJERT, 2012

[11] Vaishali T.Deshmukh, Shubhangi Vaikole, Layered Crf A Model To Build More Accurate Intrusion Detection System, IJERT, 2012

[12] Bhavana G.Rathwa,Prof.Purnima Singh Genetic Algorithm Methodology for Intrusion Detection System, IJERT, 2012

[13] Bin Zeng , Lu Yao and ZhiChen Chen"A network intrusion detection system with the snooping agents",International Conference on Computer Application and System Modeling, 2010

[14] Cheung-Leung Lui , Tak-Chung Fu and Ting-Yee Cheung "Agent-based network intrusion detection system using data mining approaches", Third International Conference on Information Technology and Applications (ICITA'05), 2005

[15] Qiang Xue , Lin-Lin Guo and Ji-Zhou Sun"The design of a distributed network intrusion detection system IA-NIDS", Proceedings of the 2003 International Conference on Machine Learning and Cybernetics, 2003

[16] Xiao-Yuan Yang , Xuan-Wu Zhou , Ping Wei and Li-Xian Wei"Hybrid NIDS based on biological immunology", Proceedings of 2004 International Conference on Machine Learning and Cybernetics, 2004

[17] Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010

Authors Profile

Mr. S K Sharma pursed Bachelor of Engineering in Information Technology from Rajeev Gandhi Technical University Bhopal (MP), and pursuing Master of Technology in Information Technology from Rajeev Gandhi Technical University Bhopal (MP).

Mr. D S Pandey pursed Master of Technology in Information Technology from Rajeev Gandhi Technical University Bhopal (MP), and working as an Assistant professor in Department of Information technology of RKDF-Institute of Science & Technology College Bhopal MP. His main focus is in the field of Data Mining and computer security. He has guided and published more than 20 research papers in various national and international journals.

Dr. V Namdeo pursed Ph.D. in Computer Science and currently she is working as Head of Department of Computer Science & Engineering and information Technology Department in RKDF-Institute of Science & Technology College Bhopal MP. Her main focus is in the field of Computer Networking, Data Mining, Machine learning and computer security. She has guided and published more than 50 research papers in various national and international journals. She holds experience of teaching over 15 years in her field

