Comprehensive study of different pattern matching intrusion detection techniques

[1]Ms. Preeti Jain (Asst. Prof.), Acropolis Institute of Technology & Research

[2]Mr. Anurag Punde (Asst. Prof.), Acropolis Institute of Technology & Research

[3]Ms. Sonu Choudhary (Student), Acropolis Institute of Technology & Research

[4]Ms. Preeti Kushwah (Student), Acropolis Institute of Technology & Research

Indore (MP)-452001, INDIA

[1]preetijn25@gmail.com
[2]anuragpunde@acropolis.in
[3]sc7058@gmail.com
[4]kushwah.preeti336@gmail.com

Abstract: Today, at very large scale the internet facility is being used by the peoples. The misuse of information, hack the confidential information of the users, confidential quotations-cash, E-banking and even in government confidential records are trying to fetch by hackers. Now we need to develope such system which detect those attacks rapidly and inform to the user. With the intention, the user will take appropriate action on their end. In this paper we have given a methodology called intrusion detection using pattern matching technique, which helps us to detect the intruders of our system as early as possible and provide security to our data. It also improved the performance of the system by nullifying the intruders on the network.

Keywords: intrusion, IDS, misuse detection, pattern matching, attacks.

I. INTRODUCTION

As the network technology is growing rapidly, the protection will become the main concerns of survival of any organisation. Today the internet is the best way to communicate, to share confidential information or to share news, credit card details, and personal information. The system's confidential information is now hard to protect due to the rapid growth in technology and extensive use of internet. The millions people are attacking to our system to heck the confidential information. The use of firewall and antiviruses will provide security but in limited manner. Now, the time comes where organisation has to think to implement the software that provide the full protection against the attacks and provide secure transmission of information within or across the network. The idea behind this is that we find the way to implement intrusion detection system (**IDS**) that provide full alert to the user over the network.

- **Intrusion:**

A set of actions aimed to compromise confidentiality, availability and integrity of computing and networking resources. An intrusion is an active sequence of related events that deliberately try to cause harm, such as rendering system unusable, accessing unauthorized information, or manipulating such information. This definition refers to both successful and unsuccessful attempts.

- **Intrusion Detection:**

It is the process of identifying the unauthorised activity takes place within or across the network and reported to the user of the system.

- **Intrusion Detection System**

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. These are SW and/or HW components that monitor the events in a computer or in a network and analyze the activities for signs of possible violations of computer security policies. Intrusion detection is not introduced to replace prevention-based techniques such as authentication and access control; instead, it is intended to complement existing security measures and detect actions that bypass the security monitoring and control component of the system. A good IDS identifies all possible intrusions and recommends actions to stop the attacks. IDS acts like a gate-keeper that will detect and block the intruder to access the network. When an intruder attacks a system, the ideal response of the system is to stop the activity. This should be done before that will damage or access sensitive information from the system.

II. Related Work

In this section we have shown the related work that has been given by different researchers and also we will give some predictions for future. This section discusses some of the works done in related area. Several data mining and pattern matching techniques are discussed in [2] - [5], [18], [19]. Authors have explained various techniques and their application in the context of intrusion detection. Authors in [6]-[8] discussed various methods for event detection and localization (location of the event occurrence). However, these schemes do not identify the events as normal or intrusive.

Pramod et al [8] proposed a system with enhanced intrusion detection capabilities. Their work includes event based video surveillance and recording, remote mapping of location for tracking and identification of human & metallic objects, support for real time surveillance and improved alarm functionalities. This system is capable of providing high detection capabilities with minimum false fails to predict the upcoming events.

Debar et.al have proposed pattern recognition techniques in [11]. The proposed work identifies and store signature patterns of known intrusions. The activities in an information system are then matched with known patterns of intrusion signatures to identify the possible intrusion. Significant matches are reported as intrusions. Pattern recognition techniques are efficient and accurate in detecting known intrusions, but cannot detect novel intrusions whose signature patterns are unknown.

Ye Changguo et al in [12] describe the wireless network intrusion detection algorithm based on association rule mining and the feasibility of the application of fuzzy association rules mining algorithm for wireless network intrusion detecting.

Ye et al [14] introduced three properties of audit data: the frequency property, the duration Property and the ordering property. They applied various probabilistic techniques for intrusion detection. In their experiments with 1998 IDEVAL data, the Markov chain based on an ordering property showed superior performance to the other techniques. This proved that the ordering of audit events assisted intrusion detections.

Gonzalez et al [15] proposed an intrusion-detection technique based on evolutionary-generated fuzzy rules. The condition part of the fuzzy detection rules was encoded with binary bits and the fitness was evaluated using two factors: accuracy and coverage of the rule. The performance of the proposed technique was compared with different genetic algorithms. Analysis was also performed without the fuzziness of rules using two network audit datasets: their own wireless dataset and the Knowledge Discovery and Data Mining (KDD) Cup 99 dataset (a small version of the 1998 DARPA dataset).

Y.Zhang et al [16] differentiated misuse and anomaly detection. Misuse detection techniques

Match patterns of well-known predefined attack profiles with the current changes, whereas in anomaly detection, the system defines the expected behavior of the profile in advance and any deviations from the normal behavior are treated as anomalies. The architecture of the string matcher based on the string matching engine described in [17]. In a string matcher, each homogeneous FSM tile takes n bits of one character (or one byte) as an input per cycle. In a state of each FSM tile, pattern identifications are stored as a partial match vector (PMV), where the i^{th} bit represents match with ith pattern. A matched pattern can be recognized after the logical AND operation of PMVs in all FSM tiles.

III.Methodology

Proposed solution is to deploy IDS which uses technique of pattern matching. This system would monitor the computer for any security breaches. IDS are the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. Pattern matching detection uses signatures or rules that describe undesirable events. They perform some action when the pattern matches an event or data. This approach allows the detection of intrusions which the system has learned their signatures perfectly. The IDS analyzes the information it gathers and compares it to large databases of signatures.

Key Benefits:

- No loss of data.
- Better resource management.
- High efficiency.

IDS application attempts to perform certain things as follows:

- In this application the user will have to sign in with username, password and the pattern he/she would like to follow for the current transaction.
- The third entity is pattern which is the new thing introduced and this is the crux of the application. These patterns will be recorded in the administrator account of the website. These patterns will be recorded and stored in the administrator account consecutively every time the user logs into his/her account.
- These patterns every time will be analyzed and matched with the previous patterns followed by the user.
- The administrator will not only analyze and compare the patterns but it will also keep track of the login and logout time parallelly.
- Small mismatch of the patterns is considerable but whenever any high mismatch between the current and the previous patterns is detected, an alert will be generated and will be provided to the user as a warning.
- The user can then take measures like changing the password etc or any other measure he/she wants to implement in the account for recovering immediately.
- Hence in this way “IDS with Pattern Matching Technique” will tremendously help in the continuously increasing network security concerns.

IV. Work done by us

Intrusion detection is the process of identifying and responding to malicious activity. An IDS performs an analysis on the information related to the internal behavior and working of the system to gain information about the security status of the target environment.

Feature Model:

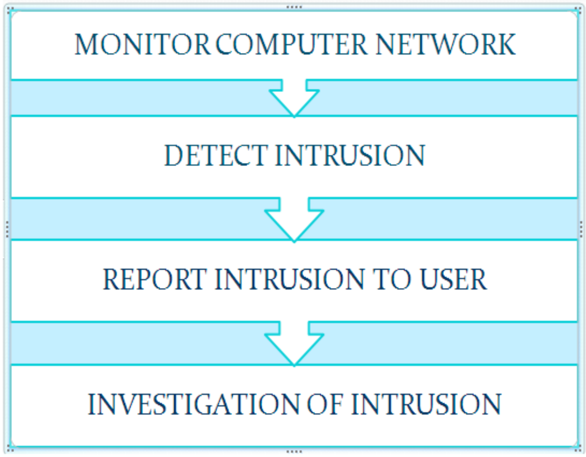
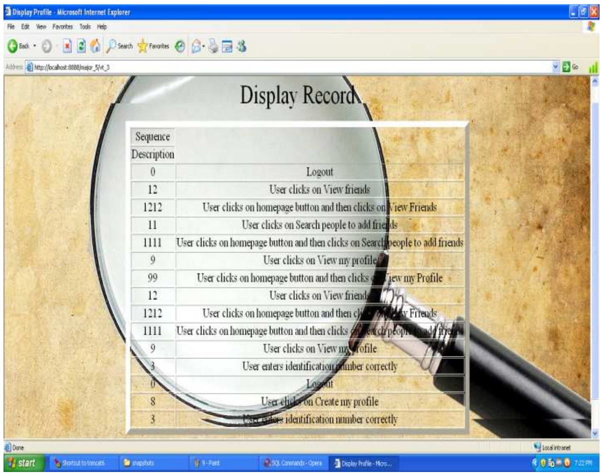


Figure 1: Model used to develope the application

Methods of applications:

- Pattern recognition
- Pattern matching
- Updating log
- Detecting intrusions
- Reporting intrusions.

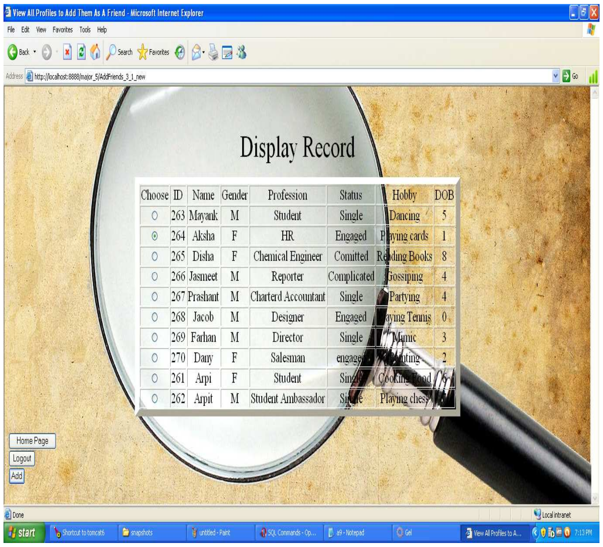
Snapshots of the application:


Display Profile - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8888/major_5/vt_3
Go
Done
Local intranet
start
Shortcut to tomcat6
snapshots
9 - Paint
SQL Commands - Opera
Display Profile - Micro...
7:22 PM

Display Record

Sequence Description	
0	Logout
12	User clicks on View friends
1212	User clicks on homepage button and then clicks on View Friends
11	User clicks on Search people to add friends
1111	User clicks on homepage button and then clicks on Search people to add friends
9	User clicks on View my profile
99	User clicks on homepage button and then clicks on View my Profile
12	User clicks on View friends
1212	User clicks on homepage button and then clicks on View Friends
1111	User clicks on homepage button and then clicks on Search people to add friends
9	User clicks on View my profile
3	User enters identification number correctly
0	Logout
8	User clicks on Create my profile
3	User enters identification number correctly

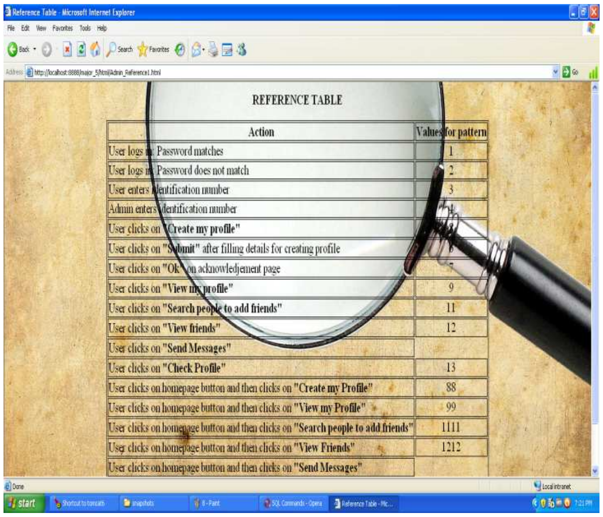
Figure 2: Sequence description used by the user.


View All Profiles to Add Them As A Friend - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8888/major_5/AddFriends_3_1_new
Go
Home Page
Logout
Add
Done
Local intranet
start Shortcut to tomcat6 snapshots untitled - Paint SQL Commands - Op... a9 - Notepad Gel View All Profiles to A... 7:13 PM

Display Record

Choose	ID	Name	Gender	Profession	Status	Hobby	DOB
○	263	Mayank	M	Student	Single	Dancing	5
●	264	Aksha	F	HR	Engaged	Playing cards	1
○	265	Disha	F	Chemical Engineer	Comitted	Reading Books	8
○	266	Jasmeet	M	Reporter	Complicated	Gossiping	4
○	267	Prashant	M	Charterd Accountant	Single	Partying	4
○	268	Jacob	M	Designer	Engaged	Playing Tennis	0
○	269	Farhan	M	Director	Single	Mimic	3
○	270	Dany	F	Salesman	engaged	Painting	2
○	261	Arpi	F	Student	Single	Cooking Food	6
○	262	Arpit	M	Student Ambassador	Single	Playing chess	[illegible]

Figure 3: Records of users


Reference Table - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8888/major_5/html/Admin_Reference1.html
Go
Done
Local intranet
start Shortcut to tomcat6 snapshots 8 - Paint SQL Commands - Opera Reference Table - Mic... 7:21 PM

REFERENCE TABLE

Action	Values for pattern
User logs in: Password matches	1
User logs in: Password does not match	2
User enters Identification number	3
Admin enters Identification number	4
User clicks on "Create my profile"	[illegible]
User clicks on "Submit" after filling details for creating profile	6
User clicks on "Ok" on acknowledjement page	7
User clicks on "View my profile"	9
User clicks on "Search people to add friends"	11
User clicks on "View friends"	12
User clicks on "Send Messages"	
User clicks on "Check Profile"	13
User clicks on homepage button and then clicks on "Create my Profile"	88
User clicks on homepage button and then clicks on "View my Profile"	99
User clicks on homepage button and then clicks on "Search people to add friends"	1111
User clicks on homepage button and then clicks on "View Friends"	1212
User clicks on homepage button and then clicks on "Send Messages"	

Figure 4: Reference table used by administrator

V. Conclusion

In our work we have try to find the patterns used by the different users and match those patterns by the patterns stored in the database. Now as per the security concerns we are generating the alert, if we found continues mismatch between the current and the previous pattern. With finding the alert the user can perform the appropriate task like changing the password. In this way this system will help the users to protect them from the intruders.

VI. References

[1]Akyildiz I.F, Weilian Su, Sankarasubramaniam Y, Cayirci E,"A survey on sensor networks", Communications Magazine, IEEE , vol.40, no.8, pp. 102- 114, Aug 2002.

[2] Dharmapurikar S, Lockwood J.W, "Fast and Scalable Pattern Matching for Network Intrusion Detection Systems", Selected Areas in Communications, IEEE Journal on, vol.24, no.10, pp.1781-1792, Oct. 2006.

[3] Ficara D, Antichi G, Di Pietro A, Giordano S, Procissi G, Vitucci F , "Sampling Techniques to Accelerate Pattern Matching in Network Intrusion Detection Systems", Communications (ICC), 2010 IEEE International Conference on , vol., no., pp.1-5, 23-27 May 2010.

[4] Nong Ye, Xiangyang Li, Qiang Chen, Emran S.M, Mingming Xu, "Probabilistic techniques for intrusion detection based on computer audit data", Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on , vol.31, no.4, pp.266-274, Jul 2001.

[5] Ke Wang, Yu He, Jiawei Han, "Pushing support constraints into association rules mining", Knowledge and Data Engineering, IEEE Transactions on , vol.15, no.3, pp. 642-658, May- June 2003.

[6] Poorani M, Vaidehi V, Rajesh M, Bharghavi, Balamuralidhar, Chandra G, "Semantic Intruder Detection System in WSN," Advanced Computing (ICoAC), 2010 Second International Conference , vol., no., pp.26-32, 14-16 Dec. 2010.

[7] Mao, Yuxin, "A semantic-based intrusion detection framework for wireless sensor network", Networked Computing (INC), 2010 6th International Conference on , vol., no., pp.1-5, 11-13 May 2010.

[8] Pramod P.J, Srikanth S.V, Vivek N, Patil M.U, Sarat C, "Intelligent Intrusion Detection System (In2DS) using Wireless Sensor Networks", Networking, Sensing and Control, 2009. ICNSC '09. International Conference on, vol., no., pp.587-591, 26-29 March 2009.

[9] [Online]. Available: http://www.antlr.org.

[10] Ilgun K, Kemmerer R.A, Porras P.A, "State transition analysis: a rule-based intrusion detection approach", Software Engineering, IEEE Transactions on, vol.21, no.3, pp.181-199,

Mar 1995.

[11] H. Debar, M. Dacier, and A. Wespi, “Toward a taxonomy of intrusion detection systems,” Comput. Networks, vol. 31, pp. 805–822, 1999.

[12] Ye Changguo, Zhang Qin, Zhou Jingwei, Wei Nianzhong, Zhu Xiaorong, Wang Tailei, "Improvement of Association Rules Mining Algorithm in Wireless Network Intrusion Detection", Computational Intelligence and Natural Computing, 2009. CINC '09. International Conference on , vol.2, no, pp.413-416,6-7June2009.

[13] R. Agrawal and R. Srikant, “Fast Algorithm for Mining Association Rules,” Proc. Conf. Very

Large Databases, pp. 487-499, Sept. 1994.

[14] N. Ye, X. Li, Q. Chen, S. M. Emran, and M. Xu, “Probabilistic echniques for intrusion detection based on computer audit data,” IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 31, no. 4, pp. 266–274,Jul. 2001.

[15] F. Gonzalez, J. Gomez, M. Kaniganti, and D. Dasgupta, “An evolutionary approach to generate fuzzy anomaly signatures,” in Proc. 4th Annu. IEEE information Assurance Workshop, West Point, NY, Jun. 2003,pp. 251–259.

[16] Mishra, A.; Nadkarni, K.; Patcha, A. "Intrusion detection in wireless ad hoc networks," Wireless Communications, IEEE , vol.11, no.1, pp. 48- 60, Feb 2004.

[17] L. Tan, B. Brotherton, and T. Sherwood, “Bit-split string-matching engines for intrusion detection and prevention,” ACM Trans. Archit. And Code Optimization, vol. 3, no. 1, pp. 3-34,

Mar. 2006

[18] Ye Changguo, Zhang Qin, Zhou Jingwei, Wei Nianzhong, Zhu Xiaorong, Wang Tailei, "Improvement of Association Rules Mining Algorithm in Wireless Network Intrusion Detection", Computational Intelligence and Natural Computing, 2009. CINC '09. International Conference on , vol.2, no, pp.413-416,6-7June2009.

[19] Hui Wang, Guoping Zhang, Huiguo Chen, Xueshu Jiang, "Mining Association Rules for Intrusion Detection", Frontier of Computer Science and Technology, 2009. FCST '09. Fourth International Conference on , vol., no., pp.644-648, 17-19 Dec 2009.