Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

The Rule Based Intrusion Detection Model for User Behavior

Zakiya Malek
Assistant Professor
GLS Institute of Computer Technology
Ahmedabad, Gujarat India

Dr. Bhushan Trivedi
Dean,
GLS University,
Ahmedabad, Gujarat India

Abstract- In this paper we propose rule based intrusion detection for user behavior. The model periodically collect the log and BIDS detector to detect normal or abnormal activity.If activity is normal then message is generated and if the activity is abnormal then the rule engine checks rules for intrusion. The malicious activity also stored in database for future IDS. The rules are stored in the rule engine of the system.

Keywords— Intrusion detection, BIDS detector, Rule engine, Expert System

I. INTRODUCTION

Intrusion detection is used to identify intrusions and intruder. Intruder may be insider or outsider. Intruders behavior different from expected users behavior.

This difference in behavior is analyzed based on which an intrusion is detected. In order to know that there is a change in the behavior of the user, audit record of the users must be maintained as input to an Intrusion Detection System.

In Rule based detection, a certain set of rules are defined that are used to identify normal user or intruder. These rules are applied to ongoing activities which then help to decide whether a given pattern of behavior is wary. The rule based detection also uses the audit records to identify the usage pattern and to generate rules for known penetration. A large database of rules are required that will cover all aspects of the known threats. These rules are to be defined such that they can detect attacks that will harm the system as well identify those activities with suspicious behavior. The rule based Expert system consist set of rules that work like human expert where analysis done of predefined rules provide by administrator or created by system automatically or both. Expert system detects intrusions using rules.[12]

II. LITRETURE REVIEW

Dorothy E. Denning, Peter G. Neumann, developed a model of an IDES that provide strong real time intrusion detection technique which detect wide range of intrusions [1]. Lunt monitored individual users, groups, remote host and overall system behavior and checks deviation between observed behavior with expected behavior, also use expert system for checking rules from the rule file [2] The Lunt IDES combine statistical user profile approach with rule -based expert system.[3]. Haystack was prototype intrusion detection system Air Force Computer Systems and detects authorized users attacks. [4] In 1992 SRI International has designed and developed a IDES learn user behavior pattern over time and detects behavior that deviates from these pattern also has a rule based component to identify known intrusions.[5]

The intrusion detection system contains information about the vulnerabilities and looks for attempts to exploit the vulnerabilities. When such an attempt is detected, an alarm is triggered. attacks) depends on the regular update of knowledge about attacks. [6] Maithili, kulkarni had implemented rule based intrusion detection and prevention model for [12] biometric systems.

III. ARCHITECTURE OF RULE BASED IDS

In the proposed system we periodically collect the different log for possible intrusions and BIDS detectors to detect normal and abnormal activity. In the given client server scenario all client log periodically send to server. BIDS detector resides on server which is create initial user behavior profile and update it if needed. If activity is normal then than message generated but if the activity is abnormal then the rule engine checks rule to check for intrusion. The malicious activity stored in the database for future intrusion detection. The rules are stored in rule engine

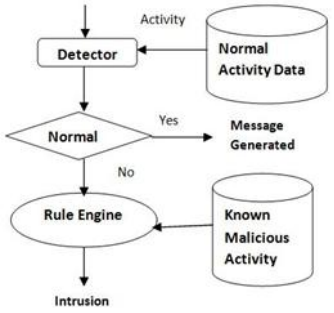

Figure 1: Components of Rule based IDS

IV. EXPERIMENTAL SET UP

We created approximately 1000 rules for different categories of users. The below figure shows hierarchy of the users for which rules and privileges are defined.

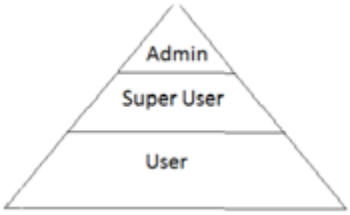

Fig. 2 (Hierarchy of Users (Bottom –Up Approach**)**

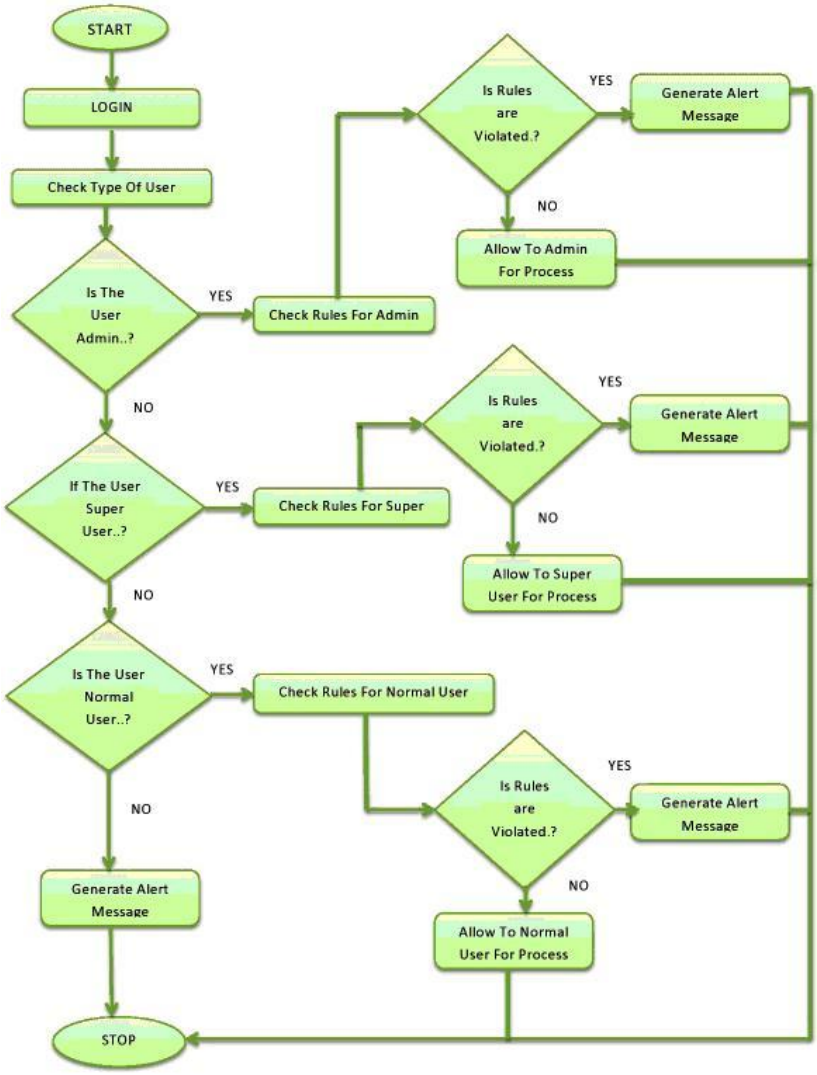

Fig.3 Flow chart of Behavior rule based IDS

In the implemented system there are rules written for different user based on their activity. Rule engine check for whether an abnormal activity is intrusive or not. We use Jess (Java based) rules. Jess rule has name, an optional documentation string, some patterns, and some actions. Here pattern is used to check for rule true or false. if rule is false then action is performed.

The rules are

```
;Intruder trying to login (defrule unauthorized-user
          (user (name ?name) {name != "shreya"} {name != "krishna"} {name != "ishani"} {name != "megha"}
{name != "anisha"}
           {name != "arohi"})
  =>
 (printout t "   U r not registered User " ?name crlf)
)
;only admin can access web
```



```
(defrule web-access-control
        (web-access {app == "chrome.exe"} {urgrp == "user"} (user ?uname)(app ?ap) (url ?url))
=>
  (printout t "   Hello, " ?uname " u cannot access web" crlf)
)
(defrule web-access-control-1
        (web-access {app == "chrome.exe"} {urgrp == "superuser"} {url == "http://" } (user ?uname)(app ?ap) )
=>
  (printout t "   Hello, " ?uname " u cannot access web" crlf)
)
(defrule owner-access
                (action {username != ownern} {usrgrp != "admin"} (username ?uname))
  =>
        (printout t " Hello, " ?uname " cannot access this Object" crlf)
 )
;authorized user trying to have unauthorized access
(defrule Aadministrator-rule-1
    " Administrator cannot login more than 2 times during working
Hours"
    (admin {login > 2} (name ?name ))
=>
 (printout t " U reached your maximum level login attempts sorry !!"crlf " you cant login anymore" crlf))
;(defrule Aadministrator-rule-2
 ; " Administrator cannot login more than 2 times during working Hours"
    (admin {login < 2} (name ?name ))
;
;=>
 ; (+ 1 ?login) ;)
(defrule unauthorized-access-superuser
        (action {usrgrp == "superuser"} {ownern == "OS"} (username ?name) (objectname ?on) )
    =>
  (printout t " Hello, " ?name " Cannot Access " ?on " as it is a system file" crlf)
  )
(defrule unauthorized-access-user
        (action {usrgrp == "user"} {ownern == "OS"} (username ?name) (objectname ?on) )
    =>
  (printout t " Hello, " ?name " Cannot Access " ?on " as it is a system file" crlf)
  )
(defrule media-player-access
        (action  {objectname  ==  "mediaplayer.exe"  }
(username ?name) )
    =>
  (printout t " Hello, " ?name " Cannot listen MUSIC in office system " crlf)
  )
Facts for intruder
;(assert (web-access (url "http://herzberg.ca.sandia.gov/index.html") (app "chrome.exe") (user "megha") (urgrp "user")))
(assert (web-access (url "http://herzberg.ca.sandia.gov/index.html") (app "chrome.exe") (user "megha") (urgrp "user")))
(assert (action (username "intruder1") (usrgrp "superuser")(objectname "system.dll")(ownern "OS")))
(assert (action (username "intruder2") (usrgrp "user")(objectname "system.dll")(ownern "OS")))
(assert (action (username "arohi") (usrgrp "user")(objectname "system.dll")(ownern "OS")))
(assert (admin (login 3) (name "shreya"))) (assert (admin (login 1) (name "ishani")))
(assert (action (username "shreya") (usrgrp "superuser")(objectname "mediaplayer.exe")(ownern "application")))
(assert (action (username "arohi") (usrgrp "superuser")(objectname "secrets.doc")(ownern "shreya")))
Facts for user
(assert (user(name "Intruder" )(usergrp "superuser"))) (assert (user(name "krishna" )(usergrp "admin")))
permission
(assert (permission (name "admin")(accessscope "RWCXM")))
 (assert (permission (name "superuser")(accessscope "RWCX")))
 (assert (permission (name "user")(accessscope "RXC")))
```


V. CONCLUSION

The implemented system is able to detect intrusions on any intranet network in which it is deployed and it should display the required information to help administrator know the type of behavior whether normal or abnormal the network is posing to the system. And also this system should be able to give all the information offline so that the intrusions that are more common to that network can be analyzed at any time.

We have used the tool named JESS-JAVA EXPERT SYSTEM SHELL,[8,9,10,11] which is a rule based engine. It has a rete class which follows a rule pattern, in that we have programmed our own 1000 rules for different types of users. Using these rules, the system will compare the behavior of the user with the rule pattern and will detect 74.5 % if the behavior of the user is intrusive or not.

VI. FUTURE WORK

In future, this system will be more enhanced and the rules will be matched according to the priority of rules defined and the after that, the rule having highest priority will be firstly detected by the system and will generate an alarm. The system will provide more user friendly interface for including rules into the rule engine. System results are stored properly in database for further check.

REFERENCES

[1] Denning, Dorothy E., "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131

[2] Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders," Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22–23, 1990, pages 110–121

[3] Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1990 Conference on Auditing and Computer Technology, SRI International

[4] Smaha, Stephen E., "Haystack: An Intrusion Detection System," The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988

[5] Teresa F. Lunt, Ann Tamaru, Fred Gilham, R. Jagannathan, Caveh Jalali, Peter G. Neumann "A REAL-TIME INTRUSION-DETECTION EXPERT SYSTEM (IDES)".Computer Science Laboratory, Harold S. Javitz, Information Management and Technology Center,Alfonso Valdes, Applied Electromagnetics and Optics Laboratory, Thomas D. Garvey, Artificial Intelligence Center, SRI Project 6784 Final Technical Report February 28, 1992

[6] SANS Institute, http://www.sans.org/security-resources/idfaq/knowledge_based.php "Jess Tutorial for Intrusion detection" http://www.cs.trinity.edu/~yzhang/teaching/spring2011/CSCI3344/projects/instruction/JESSTutor ial.htm

[7] "Jess Introduction and installation"Ernest Friedmal, Hill at Sandia National Lab. http://www.jessrules.com/docs/71/intro.html

[8] "Executing Other Jess commands and method Finding Constructor and jess.Rete methods" , Ernest Friedman-Hill at Sandia National Laboratories in Livermore, CA.

[9] "Use Jess in java (Embedding jess in java) "., http://www.jessrules.com/jess/docs/71/java.html

[10] "Making Your Own Rules ", http://.jessrules.com/docs/71/rules.html

[11] .Maithili Arjunwadakr, R.V. Kulkarni"The rule based Intrusion Detection and Prevention Model for Biometric System",Journel of Emerging Trends in Computing And Information Sciences,OCT-2010

