IJESMR
International Journal OF Engineering Sciences & Management Research

DETECTION OF BACKDOOR ATTCKS WITH GENERATING ALERTS OVER MOBILE NETWORKS

Sushama R. Borhade*, Sandip A. Kahate
*ME Student Department of computer Engineering, SPCOE, Dumbarwadi, otur,India.
Assistant Professor Department of computer Engineering, SPCOE, Dumbarwadi, otur, India.

DOI: 10.5281/zenodo.55202

KEYWORDS: Intrusion Detection System, vulnerability,Backdoor,Hashing**.**

ABSTRACT

In the today's business environment, experts must do everything to prevent network breaches. Sometimes it is very difficult to identify the attacks coming from nearly all the sides that every vector and point of entry is protected. Attack is a action that exploits vulnerability in controlled system. Recently, there has been an increase in active and passive attacks. An applications that allow for remote access to computers which is known as backdoors that are often used for targeted attacks.And to avoid these types of attack here is a new technique used in Intrusion Detection System that is JAXB technology is used to create the hashmap of complex data.

INTRODUCTION

The attack can be active when it attempts to alter system resources or affect their operation: so it compromises availability or integrity. A "passive attack[1]"attempts to read or make use of information from the system but does not affect system resources: so it compromises confidentiality.

Password Attack:

In most of the cases hackers go about stealing passwords to infiltrate a network and take access to sensitive information sush as a client database, credit card information, etc. Today, there are many ways used to break a password-protected system[2] they are as follows:

Brute Force Attack[2]: In this method third person uses possible password combinations with computer program or sript to logged into the authorized person.

Dictionary Attack: A hacker uses a program or script to try to login by cycling through combinations of common words as described in paper [3]. "In contrast with a brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a dictionary (hence the phrase dictionary attack). Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), such as single words found in dictionaries or simple, easily predicted variations on words, such as appending a digit."

Key Logger Attack:A hacker uses a program to track all of a user's keystrokes[4]. So at the end of the day, everything the user has typed—including their login IDs and passwords—have been recorded. A key logger attack is different than a brute force or dictionary attack in many ways. Not the least of which, the key logging program used is malware (or a full-blown virus) that must first make it onto the user's device (often the user is tricked into downloading it by clicking on a link in an email). Key logger attacks are also different because stronger passwords don't provide much protection against them, which is one reason that multi-factor authentication (MFA)[5] is becoming a must-have for all businesses and organizations. With **multi-factor authentication** (also called two-factor authentication, 2FA, and advanced authentication), a user is required to not only provide a password to gain access to the system, but also a another security "factor," like a unique one-time access code generated from a token device or secure mobile app on their smartphone. A network protected by MFA is nearly impenetrable to an outside attack; even if a hacker is able to attain a system password, he won't be able to provide the needed second security factor.

Phishing: There's an easy way to hack: ask the user for his or her password. A phishing email[6] leads the unsuspecting reader to a faked online banking, payment or other site in order to login and put right some terrible problem with their security[6].

Malware:A key logger or screen scraper can be installed by malware[7] which records everything you type or takes screen shots during a login process, and then forwards a copy of this file to hacker central.

Spidering: Savvy hackers have realised that many corporate passwords are made up of words that are connected to the business itself. Studying corporate literature, website sales material and even the websites of competitors and listed customers can provide the ammunition to build a custom word list to use in a brute force attack.

Backdoor Attacks:
Backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, attackers often use backdoors that they detect or install themselves, as part of an exploit.
Intrusion strategies in backdoor attacks:
Port binding: Utilized before firewalls were commonplace, port binding[12] involves specific information configurations to reveal where and how messages are transmitted and delivered within the network[8].
Connect-back: Once firewalls were put in place on many networks, hackers began using the connect-back approach, where backdoors are leveraged to connect the targeted systems[9].
Connect availability use: This strategy involves the use of several malware samples[10] to not only breach the network, but remain there undetected for long periods of time. This extends the window hackers have to steal sensitive data from the target. These are just a few attack strategies that can be carried out with backdoors. In addition, software isn't the only system that can have a backdoor. Hardware components including authentication tokens, network appliances, surveillance systems and certain communication infrastructure devices can also have malicious backdoors[11] allow for cybercriminal intrusion. Network monitoring is also key when it comes to protection from backdoor attacks. Monitoring can help guarantee that any suspicious activity – such as information being gathered by a command and control server is flagged with network administrators who then react quickly to get to the root of the issue, stop the attack and mitigate any damage.

RELATED WORK

This demonstrate how detection technology is used to construct an efficient detection system.Existing security techniques protect information systems from unauthorised access with access control mechanisms. However if access controls are compromised, an attacker may gain unauthorised access, and cause great damage in the system.Most of the existing systems have some disadvantage which limits efficiency in the detection of:Novel attacks, zero-day attacks that do not equilibrate to any previously known attack patterns or signatures.
Following table shows the ability of existing intrusion detection techniques to monitor the attack against confidentiality and integrity with examples.

Therefore, Intrusion Detection system with new technologies is the accurate identification of any set of actions that attempt to compromise the Integrity, Availability and Confidentiality of resources.The development of intrusion detection systems dates back to the early1980s by J Anderson et. al, 1980 with the publication "Computer Security Threat Monitoring and Surveillance on the various architectures of IDS systems.

Table 1: Existing Intrusion Detection Techniques.

Type	**Examples of attack**	**Type of System**							
		Application Based		**Host Based**		**Target Based**		**Network Based**	
Confidentiality	Unauthorized Access to Files and systems	-	-	Detect	Prevent	-	-	-	Prevent
	Modification of files		-	Detect	Prevent	Detect	-	-	Prevent
	Violation of corporate system use policies	Detect	-	Detect	Prevent	-	-	-	Prevent
	Violation of Security policies	Detect	-	Detect	Prevent	Detect	-	Detect	Prevent
	Weak or non existent passwords	Detect	-	Detect			-	-	
	Placement of	-	-	Detect	Prevent	Detect		-	Prevent

IJESMR
International Journal OF Engineering Sciences & Management Research

Intigrity	Trojan horse or malicious software						-		
	Presence of Trojan horse or malicious software	-	-	-	-	Detect	-	-	-
	Attack against network services	-	-	-	-	Detect	-	-	Prevent
	CGI based attack	Detect	-	-	Prevent	Detect	-	-	-

Following Figure shows the information security lifecycle .It gives the idea about the people ,process and technology in the security of the network.

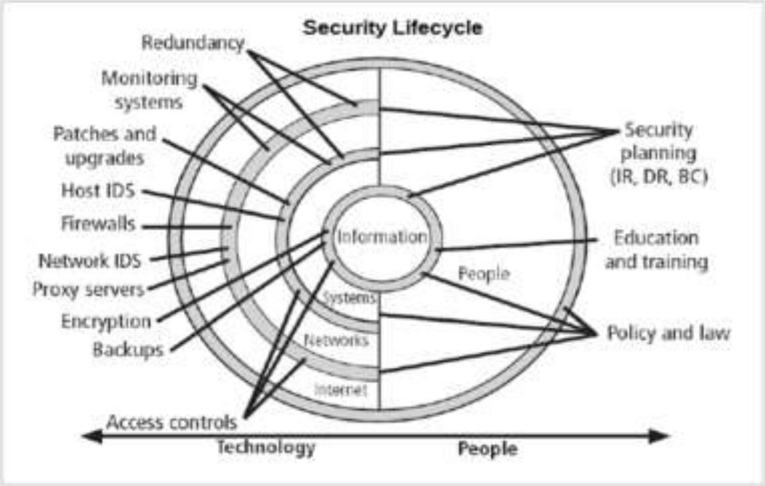


Fig 1: Security Lifecycle

SYSTEM ARCHITECTURE

The Figure 2. shows the architecture of proposed system.

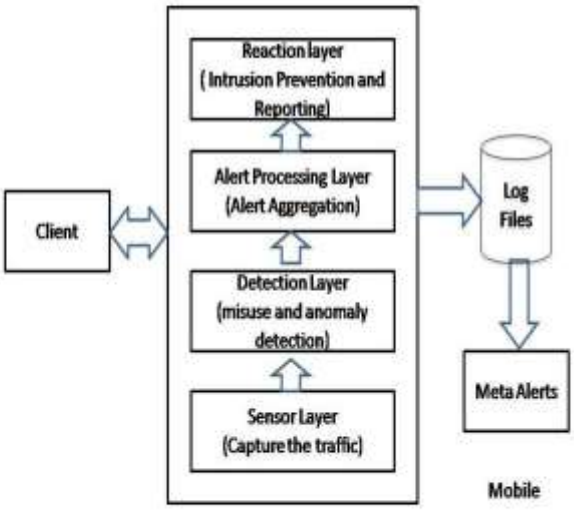

Reaction layer (Intrusion Prevention and Reporting)
Alert Processing Layer (Alert Aggregation)
Detection Layer (misuse and anomaly detection)
Sensor Layer (Capture the traffic)
Client
Log Files
Meta Alerts
Mobile

Fig 2: : Layered Model of Proposed System.

IJESMR
International Journal OF Engineering Sciences & Management Research

Here is a layered architecture of IDS from which sensor layer acts as a interface to host and the network .It takes the raw data from the host and network also then it filters the data and send to the detection layer for further processing.Detection Layer receives the data from sensor layer and using jaxb technique it matches the hashmap with the incoming data and generate the event for the next layer. Alert processing layer then generate the meta alert and forwards it to the reaction layer which reports all the attacks.

ALERT GENERATION TECHNIQUE

This section, discuss our new alert generation approach. Here a new technology jaxb i.e.Java Architecture for XML binding is used to create the hashmap which does the comparision between hashmap and the stored data to identify the violations in the stored data.

JAXB: UNMARSHALLING HASHMAP IN JAVA

JAXB allows Java developers to map Java classes to XML representations. JAXB provides two main features: the ability to marshal Java objects into XML and the inverse, i.e. to unmarshal XML back into Java objects.

JAXB mostly is used while implementing webservices or any other such client interface for an application where data needs to be transferred in XML format instead of HTML format which is default in case of visual client like web browsers.Here is a marshalling and unmarshalling of Map objects e.g. **HashMap**. These map objects are usually represent the mapping between some simple keys to complex data. , JAXB allows storing and retrieving data in memory in any XML format, without the need to implement a specific set of XML loading and saving routines for the program's class structure

The general steps in the JAXB data binding process are:

1. Generate classes: An XML schema is used as input to the JAXB binding compiler to generate JAXB classes based on that schema.
2. Compile classes: All of the generated classes, source files, and application code must be compiled.
3. Unmarshal: XML documents written according to the constraints in the source schema are unmarshalled by the JAXB binding framework.JAXB also supports unmarshalling XML data from sources other than files and documents, such as DOM nodes, string buffers, SAX sources, and so forth.
4. Generate content tree: The unmarshalling process generates a content tree of data objects instantiated from the generated JAXB classes; this content tree represents the structure and content of the source XML documents.
5. Validate (optional): The unmarshalling process involves validation of the source XML documents before generating the content tree.
6. Process content: The client application can modify the XML data represented by the Java content tree by using interfaces generated by the binding compiler

JAXB provides two ways to customize an XML schema:

- As inline annotations in a source XML schema
- As declarations in an external binding customization file that is passed to the JAXB binding compiler

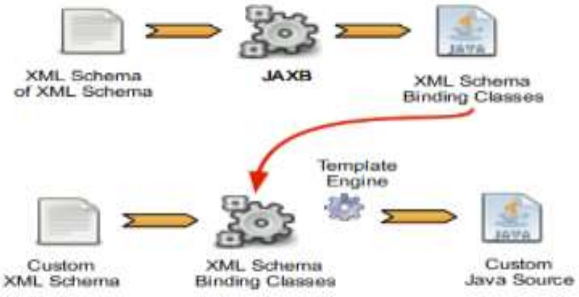
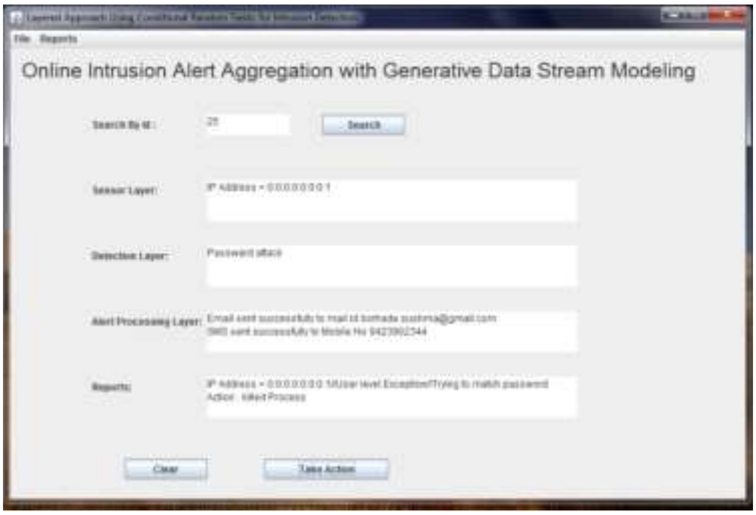


Fig 3: Java Architecture for XML binding

RESULTS

We have implemented the IDS by using java programming language. System requirement to do the implementation is JDK 1.6, Eclipse. The operating system used to do the implementation is Windows 7. We have developed graphical user interface by using swing application programming interface. Following are some user interface of Brutforce attack ,by intruder.


Layered Approach Using Conditional Random Fields for Intrusion Detection
File
Reports
Search
Clear
Take Action

Online Intrusion Alert Aggregation with Generative Data Stream Modeling

Search By Id : 25

Sensor Layer: IP Address = 0:0:0:0:0:0:0:1

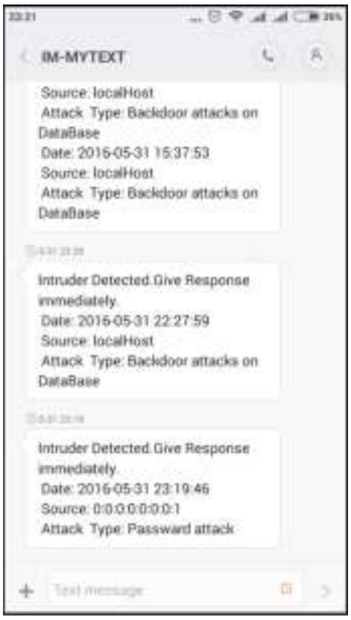
Detection Layer: Password attack

Alert Processing Layer: Email sent successfully to mail id borhade.sushma@gmail.com
SMS sent successfully to Mobile No 9423902344

Reports: IP Address = 0:0:0:0:0:0:0:1/User level Exception/Trying to match password
Action : killed Process

Fig 4: Different Types of Attacks

As shown in figure 4. attacks can be killed by the server and also inform to clients.
When violation is done in the network the appropriate action or message is displayed to users registered mobile as shown in figure 5.



Source: localHost
Attack Type: Backdoor attacks on DataBase
Date: 2016-05-31 15:37:53
Source: localHost
Attack Type: Backdoor attacks on DataBase

Intruder Detected.Give Response immediately.
Date: 2016-05-31 22:27:59
Source: localHost
Attack Type: Backdoor attacks on DataBase

Intruder Detected.Give Response immediately.
Date: 2016-05-31 23:19:46
Source: 0:0:0:0:0:0:0:1
Attack Type: Passward attack

Fig 5: GUI of Mobile Alert

CONCLUSION

Monitor, detect, and respond to any unauthorized activity are the adages of Intrusion detection systems.It allows early detection of an Internet worm making its way through a corporate network. This information could then be used to identify and clean systems that have been infected by the worm, and prevent further spread of the worm into the network, therefore lowering any financial losses that would otherwise have been incurred.This addresses the problem of accuracy and efficiency of Intrusion Detection System.It generate alerts and also by sending the Alerts as Message to the Network Administrator who governs the Network or Intrusion Detection System Department.

ACKNOWLEDGEMENTS

Authors would like to thanks all of the reserchers of the International Journals and IEEE transactions who made available their articles over the internet which helps us a lot to implement our work.

REFERENCES

1. Inam Mohammad , Rashi Pandey, Aashiya Khatoon,A Review of types of Security Attacks and Malicious Software in Network Security, International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE),Volume 4, Issue 5, May 2014 ISSN: 2277 128X.
2. Jim Owens and Jeanna Matthews, A Study of Passwords and Methods Used in Brute-Force SSH Attacks, Department of Computer Science Clarkson University Clarkson Avenue, MS 5815 Potsdam, NY 13699
3. Saikat Chakrabarti and Mukesh Singhal,Password-Based Authentication: Preventing Dictionary Attacks, Published by the IEEE Computer Society, 018-9162, 2007 .
4. Preeti Tuli, Priyanka Sahu, System Monitoring and Security Using Keylogger, International Journal of Computer Science and Mobile Computing(IJCSMC), *Vol. 2, Issue. 3, March 2013, pg.106 – 111*, ISSN 2320–088X.
5. Sugata Sanyal, Ayu Tiwari and Sudip Sanyal,A Multifactor Secure Authentication System For Wireless Payment.
6. Jyoti Chhikara, Ritu Dahiya, Neha Garg, Monika Rani,Phishing & Anti-Phishing Techniques: Case Study,International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 3, Issue 5, May 2013 ISSN: 2277 128X.
7. Savan Gadhlya,Kaushal bhavsar, Techniques for Malware Analysis, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),Volume 3,Issue 4,April 2013 ISSN: 2277 128X.
8. Pradeep Varakantham, Janusz Marecki, Milind Tambe, Makoto Yokoo,SPIDER attack on a network of POMDPs:Towards quality bounded solutions, October 17, 2006
9. Dove Chiu, Shih-Hao Weng, and Joseph Chiu,Backdoor Use in Targeted Attacks, A Trend Micro Research Paper.
10. Monika Agrawal,,Heena Singh,Nidhi Gour,Mr.Ajay Kumar,Evaluation on Malware Analysis,International Journal of Computer Science and Information Technologies, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3381-3383Vol.5(3),2014, 3381-3383, ISSN:0975 9646.
11. Byungha Choi and Kyungsan Cho,Detection of Insider Attacks to the Web Server, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 3, number: 4, pp. 35-45
12. Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),Volume 3,Issue 6,June 2013 ISSN: 2277 128X.