www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 19255-19257

APT Attacks: How Big Data Fights Back

***Rukhsana Ambreen*[1], *Prof. Shahid Nadeem*[2], *Prof. Shyam Dubey*[3]**
[1]M.Tech(CSE), Nuva College of Engineering and Technology, Nagpur, Maharashtra 441501, India
rukhsana_29@yahoo.co.in
[2]Professor, Nuva College of Engineering and Technology, Nagpur, Maharashtra 441501, India
shahidnadeem12@gmail.com
[3]Professor, Nuva College of Engineering and Technology, Nagpur, Maharashtra 441501, India
shyam.nuva@rediffmail.com

Abstract: ***Now cyber-attacks are increasing because existing security systems are not able to identify them. The cyber attacks had purposes of disclosing personal information by attacking the PC and to reduce the system. The goal of recent heavy blows. attacks has changed from disclosing information and destruction of services to attacking large-scale systems such as analytic infrastructures. The defense technologies to counter these attacks are build on patterns matching methods which are very limited. This reality, The event of new and previously unknown attack, detections rate become very low. To keep safe from these unknown attacks, which unable to identified with existing technology, We proposed the new model based on big data analysis techniques that can obtain information from a variety of sources to identify future attacks. The model base on the future Advanced Persistent Threat detection and prevention system implementations.***

Keywords: Cyber-attacks, Security systems, Intrusion detection.

1. Introduction

The past leaked personal information. This kind of attack is commonly called Advanced Persistent Threat. ADVANCED PERSISTENT THREAT aims to identified system and analyses vulnerabilities of the system for a long time. Therefore it is hard to prevent and detect ADVANCED PERSISTENT THREAT than traditional attacks and could result massive damage. Up to today, detection and protection systems for defending against cyber-attacks were firewalls, intrusion detection systems, intrusion prevention systems, anti-viruses solutions, database encryption solutions etc.

The integrated monitoring technologies for managing system logs were used. These security solutions are developed based on signatures. However, according to various reports, intrusion detection systems and intrusion prevention systems are not capable of protecting systems against ADVANCED PERSISTENT THREAT attacks because there are no signatures. To overcome this issue, security in data are beginning to apply heuristic and data mining technologies to detect previously unknown attacks.

Were Big data has been a great issue in the IT industry for the last many of years. It defines huge, shortly created and atypical data in digital environment such as text, music, video, and so on. Big data analysis is a technology that searches useful information such as a relation rule, were hidden value from huge data. Big data analysis uses various existing analysis techniques, data analysis and etc. Among various techniques, focusing on four techniques prediction, classification, relation rule, atypical . data-mining. It is means that these techniques are useful to detect unknown new attacks. The prediction is a technique that predicts the future possibility and trend. Regression analysis is a representative prediction technique. Researchers can predict attack possibilities by regressing analysis. Regressing analysis can predict behaviors from collected attack data. Second, classification is a technique that predicts the group of new attack from data. Classification helps security program to decide direction of protection and analysis. Most used classification techniques are logistic regression analysis and Support Vector Machine. In this paper, are not proposing effective parallel processing algorithm for real time analysis. Instead of using pattern matching or log analysis for predicting cyber attacks, believe that can extract valuable information status information collected from various sources by big data analysis. To apply and validate various analysis methodologies using big data, need professional software and distributed system. In future works, to implement proposed system and get results using real factors and analysis methodologies.

Due to rapid development of Internet and technology, all the machines are connected to each other either by networked system or via mobile communication. The users are producing more and more data through communication media in the unstructured form which is highly unmanageable and this management of data is the challenging job. The main focus is to gather the unstructured data from all the terminals, processed the data to convert into structured form so that accessing of the data would be easier . For this, always a track is kept on data, that this data or event belongs to which category. Accordingly, data is analyzed and processed to convert it into meaningful and right information by using the concept of Big Data Analytics. Big Data Analytics accepts the huge data sets and different data types, both half structured and not web pages, texts files or electronics mails etc. and convert it into reliable information. Big data analytics describes the simple algorithm for large amount of data without compromising performance. Analysis algorithm are provided directly to database which go beyond the pack and innovate newer more sophisticated statistical analysis. Big Data Analytics use number of tools to do the analysis and processing of data in meaningful way. Hadoop is one of the tools which is aimed to improve the performance of data processing. Hadoop is a software framework for storing and processing Big Data and work under Big Data Analytics. It is an open-source tool build on platform and aimed at to improve the performance in terms of data processing on clusters. Hadoop comprises of multiple concepts and modules to perform the easy and fast

DOI: 10.18535/ijecs/v5i11.96

processing of huge data. Hadoop is different from Relational databases and can process the high volume, high velocity and high variety of data to generate value In this paper, proposing that the use of Big Data Analytics for analyzing the enterprise data. We discussed a Enterprise data security is challenging task to implement and calls for strong support in terms of security policy formulation and mechanisms. We plan to take up data collection, pretreatment , integration, map reduce and prediction using machine learning techniques. We are developing security alerts which will provide employees with the ability to view the activity.

2. Proposed System

To establish a defense-in-depth intrusion detection framework. For better attack detection, big data incorporates attack graph analytical procedures into the intrusion detection processes. Note that the design of does not intend to improve any of the existing intrusion detection algorithms; indeed, employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise , thus preventing zombie . A cloud system with hundreds of nodes will have huge amount of alerts lifted by Snort. Not all of these alerts can be depends upon, and an effectual mechanism is required to verify if such alerts require to be inscribed. Since Snort can be programmed to develop alerts with CVE id, one proceed towards that work provides is to match if the alert is literally related to some vulnerability being utilized. If so, the existence of that vulnerability in SAG means that the alert is more likely to be a real strike. Thus, the unreal positive rate will be the joint chances of the related between alerts, which will not high the unreal positive rate compared to each individual unreal positive rate. Moreover, cannot keep aside the case of zero day attack where the vulnerability is discovered by the attacker but is not detected by computer security weakness scanner. In such case, the vigilant being real will be related to as false, given that there does not exist correlated node in SAG. Thus, present research does not inscript how to decrease the incorrect negative rate. It is important to note that security weakness scanner should be able to expose most new vulnerabilities and sync with the new vulnerability database to decrease the chance of Zero-day attacks. Rate limiting mechanisms limit the rate of packet arrivals. It is important that rate limiting mechanisms only limit the rate of malicious packets and do not harm legitimate flows. Furthermore, these rate limiting mechanisms should not incur a lot of extra over head and they shouldn't be come a source of denial of service.

we combine few concepts which are available with new intrusion detection techniques. Here to me rge Entropy based System with detection System for providing mult ilevel Distributed Denial of Service This is done in two steps: First, Users are allowed to pass through router in network site in that it incorporates Detection Algorith m and detects for legit imate user. Second, again it pass through router placed in cloud site in that it incorporates confirmat ion Algorith m and checks for threshold value, if it's beyond the threshold value it considered as legitimate user, else it's an intruder found in environment. As a result of these attacks, even though the clients expects and waits for the response from the server the server does not register its response to the clients according to their requests. This increases the infra structure response time. When the infra structure response time increases, it automat ica lly increases the resource utilizat ion. CPU utilizat ion and also time taken to create a virtual machine.

3. Algorithm

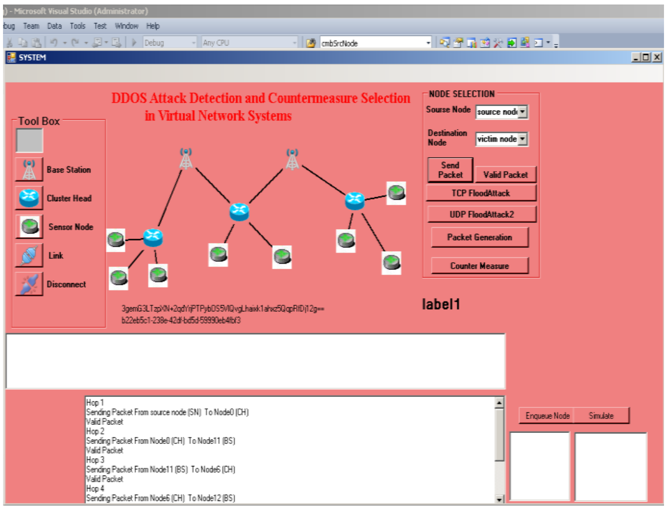
The DES and Triple-DES with improved security against power analysis attacks. The proposed designs use Boolean masking, a previously introduced technique to protect smart card implementations from these attacks. Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement.DES encrypts data in 64-bit and it is a symmetric algorithm. The key length is 56-bits.

3DES have the following advantages as encryption algorithms:

Both use symmetric keying, making them much faster at
encryption than asymmetric key encryption algorithms.

Both are easy to implement in both software and hardware when

compared to other encryption algorithms.



```
3gemG3LTzpXN+2qdYrjPTPybDS5VIQvgLhaixk1ahxz5QqpRfDj12g==
b22eb5c1-238e-42df-bd5d-59990eb4fbf3
```

```
Hop 1
Sending Packet From source node (SN)  To Node0 (CH)
Valid Packet
Hop 2
Sending Packet From Node0 (CH)  To Node11 (BS)
Valid Packet
Hop 3
Sending Packet From Node11 (BS)  To Node6 (CH)
Valid Packet
Hop 4
Sending Packet From Node6 (CH)  To Node12 (BS)
```

Figure 1 Attacks protection system

Computers become part of a zombie network through malicious software that is unknowingly installed by users or automatically installed through a security network's back door, or by exploiting web browser vulnerabilities. The malware leaves specified networking ports open, allowing computer access by outside users. Zombie networks run similar types of malware that may be multiple networks operated by different criminal entities. Types of attacks perpetrated by a zombie network include denial of service attacks, adware, spyware, spam and click fraud.

4. Conclusion

A distributed weak security detection, quantification, and countermeasure selection mechanism, which is built on attack based analytical models and network-based countermeasures. The proposed framework used to maximum advantages The network programming to build a monitor and control plane over distributed programmable virtual switches in order to significantly improve attack detection and mitigate attack consequences.

5. REFERENCES

1. Marquand, Robert; Ben Arnoldy; "China Emerges as Leader in Cyberwarfare," The Christian Science Monitor, 14September2007, -woap.html
2. Rain; "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspec tive," Proceedings of the 7th European Conferences on Information WR-fare, Plymouth, 2008
3. Brewin, Bob; "U.S., British officials target Chinese as Source of cybe rattacks," Gover n-ment Executive, 4 December 2007, www.govexec.com/defense/2007/12/us-british officials target chinese as source of cyberattacks/25874/
4. Clayton, Mark; "US Oil Industry Hit by Cyberattacks: Was China Involved?," The Chri tian Science Monitor, 25January 2010, www.csmonitor.com/USA/2010/0125/US
5. Samuel, Henry; "Chip and Pin scam 'Has Netted Millions From British shoppers'," The Telegraph, 10 October 2008, www.telegraph.co.uk/news/uknews
6. Drummond, David; "A New Approach to China," Google Blog, 12 January 2010, http://googleblog.blogspot.com/2010/01/new
7. A.K.Sood, R.J. Enbody "Targeted Cyber attack: A superset of advanced persistent threats" Security & Privacy, IEEE Volume 11 Issue 1, pages 54-61, Jan-Feb, 2013.
8. Apache Hadoop Project http://hadoop.apache.org/
9. "Hadoop Tutorial from Yahoo!", Module Managing HadoopCluster.http://developer.yahoo.com/hadoop/tutorial/module7.html#machines
10. K. Shvachko, H. Kuang, S. Radia and R. Chansler, "The Hadoop distributed file system", in poc. The 2010

IEEE 26th Symposium on Mass Storage Systems and Technologies (MMST) 2010.

11. F. Cuppens and A. Mige, Alert correlation in a cooperative intrusion detection framework, in Proc. IEEE Symposium on Security and Privacy, Berkeley, California, USA, 2002, pp. 205-215.
12. A. Hofmann, I. Dedinski, B. Sick, and H. de Meer,

A novelty driven approach to intrusion alert correlation based on distributed hash tables, in Proc. 2007 IEEE International Conference on Communications (ICC), Glasgow, Scotland, 2007, pp. 71-78.

13. B. Mu, X. Chen, and Z. Chen, A collaborative network security management system in metropolitan are a network, in Proc. the 3rd
14. International Conference on Communications and Mobile Computing (CMC), Qingdao, China, 2011, pp. 45-50.