International Journal of Research in Advent Technology, Special Issue, NCRCEST 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Catching The Threats Inside The Organization

[1]Nilesh Jain, [2]Nikhil Kumar Singh, [3]Prasoon Gupta,[4]A.Arulprakash,
[1,2,3]Student of Computer science Department, Galgotias university,
[4]Professor in Computer science Department, Galgotias university
[1]Nilesh.99jain@yahoo.com, [2]nksingh82077@gmail.com,
[3]prasoong16@gmail.com, [4]prakash875@gmail.com

Abstract: This paper deals with all the proposed ways to solve the problems that arise due to the insider attacks detected in the research history of Computer Security. The basic idea of this paper deals with the differentiation between two different cases of insider attack; The Masquerades and The Traitors. The challenges faced due to these insider attacks have been described and the approach towards the solution of these with NextGen techniques pursued by the research organizations to barricade all such dirty-dealing. The paper is going to deal with all the future research, the problems, the solutions and the human era exploiting their employer establishment.
Keywords Insider Attacks, Computer Security, The Masquerades, The Traitors, NextGen Techniques

1. INTRODUCTION

As per a 2018 report by CA Technologies, the most threatful security loopholes are no more induced from outsider attacks; Malicious Outsiders or Malware but originate from the Malicious Insider or the ones considered as Negligent Insiders. The report was a result of a survey which gathered information about all the latest trends and challenges faced due to insider threats. They have not just covered challenges faced but also the solutions to prevent or extenuate insider attacks.

Their community comprises of a huge 400K online members, Cybersecurityanalysts in collaboration with the Information Security

Community on LinkedIn which in order to obtain a report persuaded Crowd Research Partners to conduct a core study by Cybersecurity Security Professionals which collected fresh analysis on different parameters and published the latest trends and provided with much required guidance to vanish insider attacks.

This INSIDER THREAT report has been considered as the most in-depth case study on the topic till date, exposing how Information Security and Security Professionals are fighting with the perilous insiders and how the organizations are preparing to protect and preserve their valuable and critical data along with their IT Infrastructure.

1.1.The Major Conclusions of This Survey

1.90% of organizations consider themselvesvulnerable to insider attacks. The main risk factors are too many users with unwanted access privileges (37%), a growth in number of devices with access to sensitive and valuable data (36%), and the increasing complexity of IT (35%).

2.A majority (53%) of organizations has confirmed insider attacks against their organization in the last one year (typically less than five attacks). 27% of organizations say insider attacks have become more frequent and are getting powerful day by day.

3.Organizations are focusing on detecting insider threats (64%), followed by deterrence methods (58%) and analysis and post breach forensics (49%). The utilization of client conduct checking is quickening; 94% of associations convey some technique for observing clients and 93% screen access to touchy information and significant information.

4.The most prominent advances to stop insider threats are Data Loss Prevention (DLP), encryption, and personality and access the board arrangements. To more readily recognize dynamic insider dangers, organizations convey Intrusion Detection and Prevention (IDS), log the board and SIEM stages.

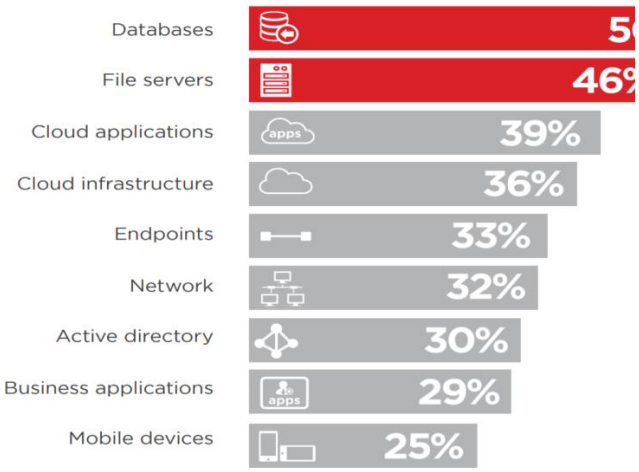
5.The larger part (86%) of organizations as of now have or are building an insider threat program. Thirty-six percent have a formal program set up to react to insider assaults, while half are centred around building up their program.

2.NATURE OF INSIDER ATTACKS

The are major misconceptions related with the term “INSIDER ATTACKS” or “INSIDER THREATS” in cyber security is that the employees within the company are the Masqueraders and the traitors harm the company directly by stealing the data or sabotaging it. At times, they are the culprits but the foremost attacker goes unobserved which cause high number of security breaches and leaks intentionally or unintentionally.

2.1.Computer Security The cyber specialists have the ability to detect, counter and dodge cyber-attacks. The job never goes easy on them, new challenges are faced each day with the advancing technologies and moreover when the attacks are from within the organization from the trusted and Access granted authorized personals. The job of the cyber specialists becomes more tough because it is very tough to find whether the employee is doing his normal routine work or planning a masquerade.

2.2.TheDiamond Data is considered the diamond of the IT company; it’s core asset and the data might have different worth depending upon the secrecy and the use of it. Blueprints of the organization, confidential business data, company financials and the personal data of the partners and employees, is an asset towards which no organization takes risk when it comes to the security of it.



These IT assets are most vulnerable to INSIDER THREATS.

3.DETECTION OF INSIDER THREATS

It is necessary after a case study on such a sensitive topic to find solution to avoid and dodge such loss.

3.1.Host Base User Profiling Let's take an example of generalized condition to better understanding, after an attack or a crime designated personnel are deployed for investigation of situation and crime scene and then the same is forwarded to upper-sub- ordinate divisions.

Similarly, cyber-attacks are handled by examining different sources of errors and flaws, although it is a slow and hard process but it is worth result. The investigation or research or audit is broadly distributed in some phases that can be-

1. Command lines issued
2. System call for unusual activities
3. Database inspection
4. Organization policies and compliances

This all reports and inspections are then processed for finding an attacker, but sometimes this much of data is insufficient for providing a solid output report by which investigations should be processed, then a deep investigation work is deployed and line by line is processed for finding the flaw which lead to attack and counterworking on it.

3.2.Investigating And Fabricating In

on Windows is way too less then Unix and Linux environment.

Even though a significant amount of time, money and labor has been invested in algorithms for their generation, execution and inspection but no applaud able results has been announced.

Windows server 2000 was prone to some issues but after that various versions and patches been applied so it is becoming a hard task to attack from Windows environment. We've travelled a long distance and also proved a good way to tackle problems and issues.

However, in any worst case, let's assume a Windows environment responsible for attack to an organization or an institute. It is practically impossible to inspect every line of code form windows environment command line as it generates an enormous number of code throughput.

3.2.1. Investigating and fabricating in Web environments-Web environments provides best for an attack and also helps a lot in covering tracks. Attackers usually generate anomalous amount of request which is then pinged to an attack location. Being a huge amount of request, it practically and logically becomes impossible for filtering and checking every request report.

After execution of malicious code and introducing malwares the attacker can easily get away just by clicking a single "Log-Out" button. As a single connection it can also be sometimes difficult to find source as change in user behavior.

3.3.Network Based Sensors

3.3.1. Network observable user actions-In past many of surveys with anonymous users those who claim to have sufficient and specific knowledge for breaking into a network and also in many cybersecurity workshops and meetings, they stated that in an attack it is not mandatory to enter in a network with wrong intentions. After gaining sufficient access privileges and knowledge of environment a small loophole or flaw may be exploited for damage and destruction, greed for money.

5 malicious scenarios were replicated and some protocols were also specified to be violated. **Unix/Linux Shell**-Before proceeding forward, we have to know about Markov Chain or more importantly hybrid high-order Markov Chain. It is a discrete-time stochastic process, and is used for signatory-behavior of user, it uses mixture transition distribution approach for carrying tasks.

Another detection method deployed is called uniqueness which works on fact that commands passed are unique and of some use and it also filters useless command that are irrelevant of situation and provides useful and gives helpful support.

Although there are various algorithms and method to find out suspicious chain of commands and raise an alarm beforehand so that attack may be sabotaged but using them also leads to a massive false alarm also. So sometimes in order of avoiding the false alarm the true alarms are also ignored which in turn proves to be an attack.

3.3.2Investigating and fabricating in Windows command line-An important point to be discussed, Windows is some-where unable to provide the amount of destruction as compared to Unix and Linux environment. Therefore, the amount of work implied After successful operation of replication some sample data were collected from the organisation that suffered attack which were mainly HTTP, SMB, SMTP and FTP but nothing unusual was monitored in the sample data which made it hard to investigate the attack even data traffic throughput was normal no major hikes were observed.

Therefore, organisations have to keep working on their network and data structure to rectify any flaw or loop-holes before letting any personnel in network. The person having charge of modifying network should know information about network on 'need-to-know' basis. Information's and briefs should be released as and when require instead of handing an entire handbook and guide of network and electronica infrastructure.

3.4.Honeypots Honeypots are internet-based system which act like a source of information but in reality, they attract intruder and attacker. Honeypots are programmed to copy systems that an attacker would like to chase into but restricts attacker to only a part of system and infrastructure. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored.

Almost all honeypots are camouflaged inside firewalls so that they can be controlled physically or remotely, though it is possible to install them outside of firewalls.

By luring a hacker into a system, a honeypot serves several purposes:

- The organisation can watch the attacker exploit the weaknesses and loopholes of the system, thereby understanding where the system has weaknesses that need to be reinforced.
- The intruder can be caught and restricted while trying to obtain root access to the system and privileges.
- By studying the steps and tactics of attacker, developers can develop betterand can create more secure systems that are potentially invulnerable to future hackers.

Honey Net is a network of honeypots.

3.4.1. Integrated Approaches Integrated approaches define multiple barriers for an authority to cross. Physical security logs are maintained in case of any mishap for some effective investigations. This also defies multiple access points such as honeypots, firewalls, RAS (Restricted Access Systems) to cross and enter in security clearance guided system.

Moreover, in fact this system was deployed in various organizations across globe for better security and avoiding insider attack but it turns out failure and now it is not able to keep up with systems and users' throughput.

4.SUMMARY

So, now summarizing the entire work and will be stated as,Insider attacks are usually performed by a single individual or group of individuals having sufficient knowledge of network and data infrastructure. Linux and UNIX attacks are easy to trace back for an attack while Windows environment prove it hard to track back. On the other hand, web environments provide an easy and friendly base for an attack.

Countering the attacks, organizations came up with some golden ideas to work on them, they replicate attacks to study, investigate and counter it. Some of it came to be a great success such as Honeypots (luring attackers into a trap), providing only 'need-to-know' information and employees so they can access up to a certain level in infrastructure.

Multiple barriers are also deployed in a network and physical logs were also kept for better understanding and working of command, data traffic throughputs were monitored closely but none of them proved to useful. As we speak the environments and machines are being developed in a way so they can't be traced and are able to camouflage in vast pool of data and network. They are like transparent film in a strict vigilance and disappear to no-where.

5.FUTURE RESEARCH DIRECTION

One of the popular means through which one can identify abnormal user behaviour for masquerade attack detection is user profiling. Abnormal behaviour here is consider as good hint moreover an indicator towards the identity theft .user profiling can used for other purpose such as traitor detection. Profile model is needing now a days and will a major role in future too. it will provide us with the information about the any intent or suspicious and malicious action. It may not be enough as concluding a malicious act barely knowing that a user has issued a command which is abnormal unless that command breaks or violate any security policy. major loop hole of insider attack detection is the lack of data provided as in order to study and to conclude one must need a proper data over it before providing the general solutions but that is not the only problem with insider attack detection another problem is that it is quite a hard job ,if not impossible to get the source and the data from the traitor while the masquerade is performing their malicious activities .real intrusion is hard to obtain for ground truth test and evaluating as attack might be mistaken or firms might not admit their crime and hence they will avoid and will not cooperate another reason is that researcher on general bases do not have sufficient data as well as the are not able to directly access to the real attack.

Various programs and software came it action to get rid of the problems and loop holes discussed above one of such software is RACOON which helped in creation of user command data from anonymous detection from templates which are customizable representing particular user profile. capture the flag exercise also came into action and helped in creating and generating insider attack database which are nature wise realistic and can also provide us with a means of advance state of the art which will finally lead us for the better understanding of the insider attack further we can say that it will help us in solving the problem of insider attack. Biggest problem faced by researchers is to detect accurately between the cases where in the first case is that when the insider attack is verified with high percentage and the second case in which the insider attack is ignored or inferred with partial knowledge, lack of data and information. making a difference between false positive and true positive in presences of uncertainty is quite a challenging task. it became more of a hard ache when people's reputation is on stake. Therefore, any technology developed for the detection of insider attack must include strong privacy preserving guarantees for the purpose that will help in avoiding the false claim because such claims can harm the reputation of the individual and the organization. A proper trap is need for trapping traitor's behaviour and it is quite hard to compute the accurate user profile efforts has to made for developing a technique moreover trap which will help us in finding the accurate profile and the traitor red handed. Another problem which has to be addressed here is that how can one develop a trap for those who have the knowledge and are aware of it. things will be sophisticated if the traitor is already aware of the trap and the technology in

use. Another thing which can be enlighten here is the investigation of alternative mitigation strategies.
For example, how the machine works in the department of monitoring and detection of the threat and how it challenges a user when detection process is complete after which the system conclude that the task performed comes the malicious activity. Question which gets a hike here is that how is it possible to stop the attack without disclosing the details of the employee's true identity unless and until his / her act violates the security policy. another problem is that the amount of data varies a lot it is not fixed that how much of data is required for modelling process nor the tie duration is fixed how long should one must collect the data which will be enough to build a data set which afterwards will leads to towards the insider attack detection and disclosing the traitor only thing which might reduce the chances here is the accuracy whether the data set result will provide us with a percentage confident enough to put claim on the traitors action regarding the malicious activity he / she was involved in or rather performing .

6.CONCLUSION

Insider attack detection is an open opportunity in the field of research and development for new approaches new methods and research ideologies. A bulk of algorithm modelling and machine language is available as well as a rich audit source is also available that can be used and acquired effectively. however, the slim possibility which comes with it to create something very effective with an accuracy of nothing less than a hundred percent with automated accuracy and monitoring for detecting the insider attack. developing something like that is still an open challenge. Scarcity of ground truth data limits the value of various solution proposed since accuracy still remains the problem as it is hard to measure or calculate the validity of the method proposed. various method was proposed evaluated and the conclusion was that the dataset is useful to compare between the computational performance and competing algorithm, still here also accuracy is not measurable it can vary. a number of methodology and approaches were taken into consideration later they all get neglected with the words "subject of considerable future research and development". Various surveys were conducted on different modelling algorithm and machine language applied to traitor attack detection using two different kind of audit sources namely they are host-based audit sources and network-based audit source however the results concluded that the best audit source one should use automated machine to detect the traitor or masquerade is still not known. the approach of experimental methodology is also failure too as the major problem which arises in that methodology is lack of suitable realistic data. many methodologies came it consideration and various methods were proposed but their utilization was uncertain and none of them were superior from other. Detection based on trap, use of decoys technologies and honeypots of different types were partially explored. by far the summary here ends with a questionnaire conclusion that the insider attack detection by a masquerade or a traitor still remains as an open opportunity, an area still to be explored in the field of research and development.

REFERENCES

[1] Spitzner L, Honeypots: Catching the Insider Threat. ComputerApplications Conference, 2003.
[2] The Honeynet Project "Know Your Enemy: Credit Card Fraud", 10 July, 2003. http://www.honeynet.org/papers/profiles/cc-fraud.pdf
[3] The Honeynet Project "Scan of the Month Challenge 28", May 2003. http://www.honeynet.org/scans/scan28/
[4] The Honeynet Project "Know Your Enemy: Honeynets", January, 2003. http://www.honeynet.org/papers/honeynet/
[5] Lance Spitzner "Honeytokens: The Other Honeypot", August, 2003. http://www.securityfocus.com/infocus/1713
[6] The Honeynet Project "Scan of the Month13" March, 2001. http://www.honeynet.org/scans/scan13/
[7] V. Yegneswaran, P. Barford, J. Ullrich, "Internet Intrusions: Global Characteristics and Prevalence." In Proceedings of ACM SIGMETRICS 2003, San Diego, CA, June 2003.
[8] John Levin, Richard Labella, Henry Owen, Didier Contis, Brian Culver, "The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks", IEEE Proceedings, June 2003. http://www.tracking-hackers.com/papers/gatechhoneynet.pdf
[9] Malek Ben Salem, ShlomoHershkop, and Salvatore J. Stolfo, A Survey of Insider Attack Detection Research, Computer Science Department, Columbia University. (2008)
[10] John Levin, Richard Labella, Henry Owen, Didier Contis, Brian Culver, "The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks", IEEE ProceedingsAvailable: http://www.tracking-hackers.com/gatech-honeynet.pdf.