International Journal of Engineering Research in Computer Science and Engineering Engineering (IJERCSE) Vol 2, Issue 3, March 2015

# A Technical Monitoring Tool to Mitigate Insider Threat under Windows Environment

[1]Ashokkumar G,[2]Prof. S. Rajendren
[1]M.Tech -Information security and cyber forensics, SRM University, Kancheepuram Dist., TamilNadu
[2]Department of Information Technology, SRM University, Kancheepuram Dist., TamilNadu
[1]ashok_gnanasekar@srmuniv.edu.in,[2]rajendran.s@ktr.srmuniv.ac.in

.

*Abstract* — **The insider vulnerability assessment and threat identification based on event logs and security monitoring for windows network machines assist in the internal threat identification of an organizations. It is the process of tightening the security measures and active monitoring of activities for their internal employees. The Organization's Security analyst can assign the severity levels and their ranks to automate the security alert information and monitoring. The add-on features for restriction setting and user activities monitoring are particularly essential for monitoring threats inside the organization. The dynamic nature of security requires facilitated windows batch and PowerShell commands execution in the same platform for the security analyst.**

**Index Terms — windows insider-threat mitigation security analyst, survey.**

## I. INTRODUCTION

IT Organizations even the security product companies more prone to Insider security threats because of various motivating factors. The motivation of disgruntled employees may range from personal benefits, espionage, ignorance etc. In many cases, there are securing of the system and monitored security for the insiders in any organizations can cause serious of losses and prevent the growth of the particular unmonitored or unsecured organizations. Specifically refers to the users of an information system exploiting their legitimate access rights to that system, in order to perform malicious acts.

Attacks launched from inside organization network has intense level of threats, especially in case the attack performed by person within the network. It is easy for any attacker working inside the network for gaining administrative access and permissions than the outside attacker. The account misuse, privilege escalation may case serious problem to security of the organization. The internal network sometimes suffer because of lack of maintenance activity on accounts that offer possibility for attackers to carry out with in the network of leaving the account active of a former employee which the insider use to intrude by masquerade to perform illegal activities etc. Sometimes, huge availability of information within the network machines may cause serious security problems. In situations, organization may undergo serious data theft problems.

The theme of this paper is from the CERT. The reports on internal threats based on data collected from real cases. The CERT research offers valuable measures for increasing security for mitigating the internal threats. The lack of measures in adopting the standard methods may cause more chances of attacks in internal network by the insider. The

countermeasures are mandatory for preventing such attacks. The Microsoft offers the standard policies and frameworks for maintaining the security on the machines running their windows operating system.

## I. MITIGATING INSIDER THREATS BY ACTIVE DETECTION

The event log collected from various machine used to gain traces to gain information on malicious activities performed by the insiders of an organization in a standalone or network computer. The framework service that run in windows collect log information at some time intervals regularly and updates about the events for suspicious activity. The logs collected in the database of the framework used for active detection of threat.

A number of sources in the literature posit that insider incidents are not reported on every time of it occurrence. Roy Sarkar [4], for example, offers four reasons, from the perspective of the organization for insider incidents not reported because of fear of negative publicity; difficulty identifying culprits;

ignorance of the attacks; overlooking incidents due to low impact. Colleagues of a malicious insider may notice suspicious activity, but not report what they have seen. The solution to this issue is providing security by continuous monitoring of user activity. The windows machines connected in the network run in surveillance mode to monitor the activities of the user.

The data theft monitored by timestamps of files and folders. The threat assessment run by the security analyst facilitated with filtering facilities especially of internal threats related vulnerability identification options.

The filters can applied to the event logs to maximize the chances of finding attacks that are within the inside the network connected machines. Malicious activity meter reports the severity level and measures to enhance the security to the user.

*a) Non-Technical Prevention*

The neutralization techniques that actively reduce intentions of users to violate security policies, developing the situational Crime Prevention. The various methods of prevention include implementing the MERIT model offered by CERT and following regulatory standards for mitigating the insider threat like mentor, proper education to the employees can considerably reduce the risk of internal threats.

*b) Technical Detection*

This subcategory cover mechanisms that review access in terms of fulfilment of security obligations, file access monitoring, internal webserver log monitoring, frameworks that leverage multiple log sources for detection, host-based monitoring and network flow analysis technologies. The early detection of abnormal inside user activity may save billions of dollars for the organization. The continuous monitoring analysing of event based on the vulnerable events reports the incidents of threats anywhere within the environment. Although there is some third vendor solutions that exist solving some issues but that are not designed for insider threat mitigations and monitoring.

## II. TECHNICAL PREVENTION

This category covers early warning systems based on the traditional system configuration checking for stability and reliability of the system. Correlating and mapping of organization policy with windows group policy settings can help in the mitigation of insider threats. It helps in classifying the permitted and denied permission standards and assist finding the most relevant vulnerability that may reside in the system. The log collection involves various Microsoft event logs for analysis. The early detection of abnormal inside user activity may save billions of dollars for the organization.

The continuous monitoring analysing of event based on the vulnerable events reports the incidents of threats anywhere within the environment.

*A. Event Logging:*

All versions of Microsoft Windows and later, are able to record security events using built-in log file functionality. In a Microsoft Windows–based environment, this functionality provides the basis for security monitoring. There are two types of events in the Security event log analyser namely, success audits and failure audits. Success Audit events indicate an operation that a user, service, or program performed successfully. Failure Audit events detail operations that have not completed successfully. For example, failed user logon attempts would be examples of Failure Audit events and records in the Security event log if logon audits enabled.

*B. Logs Analyse:*

Event logs contain entry for activities of events in the machine. It helps address both internal and external threats. Careful analyses necessary for tracing the evidence of crime inside the organization. Security Event logs provide facilitates to incorporate detection mechanism to the framework operation. Apart from security audit logging various other logs are possible to create on Microsoft window operating system. All versions of Microsoft Windows until the recent versions follow the event creation categories on system, application, and security. However, internal threat detection requires log manipulation from the collected log records. It is not available as a build in functionality for performing forensics analysis on internal threats. Insider Threat activity analyse and detection in monitoring mode covers the tracks of the inside attacker activity on timeline basis. This report will help in proactive detection rather than solely for reactive forensics. Also most attackers, attempt to cover their tracks by altering logs; therefore, continuous monitoring and storing of logs provides logs information intact. This mechanism turns out that logging and activity detection is a vital tool in the network security arsenal if used and secured correctly.

System logs monitoring on the internal network is the core security monitoring and attack detections mechanism for most problems of internal threat identification. Other issues associated are identifying and remediating systems that are not compliant security policies i.e. finding the rogue machine and user of the

machine and alerting. System stability relied on recommended vulnerability patches, so any problem with system update are essentially important for monitor. Internal network infrastructure monitoring also includes open ports and services of the windows system.

*C. Event Filtering based on Threshold value*

An Audit checklist for users are different based on role of the employee the roles are not same. Therefore, performing auditing yield information that can be useful for monitoring. For example, different type of audit log monitored is configurable depending on the nature of organization and role of the user. The Users mapped with the type of audit logs for collecting the relevant information on inside attacks. The event type can be security focused or activity focused. The suspicious events from the collections filtered based on severity level, Time and date, occurrences parameters. The parameters help in security analyst valuable information for taking counter measures.

*D. Identifying Security Policy Violations*

Correlating security event information involves the collection of security events from multiple systems and the placement of this data into a central database location. When security information correlated, the appropriate personnel can analyse this central repository to identify violations or external attacks. This repository is not only important for forensic analysis, but also as a tool to detect attacks and address vulnerabilities. Although there are several third-party solutions that exist for this purpose, the Microsoft Script tool can help address this need by correlating security event logs and other security monitoring information into a central repository.

## III. DATA THEFT PREVENTION

Data Theft prevention includes setting restriction and outbound limitations on various data leakage supporting network technologies including ftp, tftp, ssh and technology devices like USB, printer, CD/DVD Drives, Mail. Limiting access is just one of the steps to secure data; preventing copying is the next step in securing internal access.

*A. USB Access:*

The ports available for transferring the data or connecting the USB mass storage devices should configurable to block during restricted time of access on the machine or in time need of permanent block. USB storage devices can hold large volume of data in case misuse of the property inside the organization can create even data loss at great levels. Port monitoring will assist actively and it detects a new hardware ports with the windows system and alert to the system administrator and analyst.

*B. DVD/CD:*

The DVD/CD comes under one of the potential dangerous devices in the case of data theft. The scenario like if it is for presentation, this should conducted in controlled or designated machine.

## V. ACCESS RESTRICTIONS

Many organizations have a relatively liberal policy on access restrictions with folder open permissions to various department and persons. The data for confidential storage are compartmentalized and employees should able to access data that need for their job. One-step higher level of biometric security adoption is most preferred for strong prevention of DLP (Data Loss Prevention). The insiders within the organisation should not share their passwords with any one for confidentiality of secure access to sensitive data. The treatment for data loss prevention includes biometrics, automatic desktop lock after few minutes of user inactivity noticed by the system. The data theft protection provides way to create directory and folders with special parameter attributes. The folders will be hidden from access by the insiders. Access to group policies editing and registry editing options on the windows machine should be restricted access to the internal employee.

## CONCLUSION

In this paper, I have analysed and identified threat causes and their scenarios in the organization that incorporated Microsoft windows operating system based platform. I have also tried to my detection mechanism by extending the capabilities of the existing software and script support including the recommended tasks that necessary for preventing the particular functionality and operation. Since my package can proactively detect the insider's goal is achieved the organization can detect the malicious activity before it is already diseased. I my future work I believe that much enhanced features like scan detection, traffic detection into the internal threat detection-monitoring environment in order to increase the detection mechanism. The ultimate moto of this project will continue with the motivation advancement and almost very easy to use environment for the end users.

## REFERENCES

1. Mitigating Insider Threats by Active Detection. Journal of Modern Internet of Things. Joon S. Park, Jaeho Yim, Jason Hallahan (2013).
2. The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24(6), 472-484. The oharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005).
3. Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report, 15(3), 112-133. doi:10.1016/j.istr.2010.11.002. Roy Sarkar, K. (2010).
4. Understanding Insider Threat: A Framework for Characterising Attacks. 2014 IEEE Security and Privacy Workshops. Jason R.C. Nurse, Oliver Buckley, Philip A. Legg, Michael Goldsmith, Sadie Creese, Gordon R.T. Wright, Monica Whitty.
5. Defining and Analysing Insiders and their threat in organization. 2011 IEEE. Alawnch M, Abbadi I.M.
6. Use of Domain knowledge to detect Insider threat in computer activities. IEEE security and privacy workshop. Frank L.Greitzer, Thomas A,Ferryman.
7. Reflecting on the ability of enterprise security policy to address accidental insider threat. IEEE Security and Privacy Workshops.
Oliver Buckley, Jason R.C Nurse, Philip A.Legg, Micheal Goldsmith, Sadie creese
8. Use of domain knowledge to detect insider threat in computer activities. IEEE Security and Privacy Workshops. Young W.T, Goldberg H.G, memory A.
9. Trust Enhanced Security Architecture for detecting insider threats. 2013 IEEE Security and Privacy Workshops. Tupakula U, Varadharajan V.
10. A descriptive Literature Review and Classification of Insider Threat Research. 2014, Proceedings of Information Science & IT (InSITE). Jacques ophoff, Adrain Jensen, Sanderson smith, Micheal Portwe and Kavin Johnston.
11. The Insider threat to information system and the effective of ISO 17799. 2005, ELSEVIER. Marianthi Theoharidou, Spyros Kokulakis, Maria Karyda, Evanelog.
12. Insider Threat Attributes and Mitigation Strategies by George J. Silowash. Link: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1739&context=sei
13. International Implementation of Best Practices for Mitigation Insider Threat: Analysis for India&Germany.Link:http://resource.sei.cmu.edu/asset_files/TechnicalReport/2014_005_001_88427.pdf