Behaviour Analysis of Client Side Cyber Attack

Aditya Bhople[1] Aayuka Nirawade[2] Sanyam Patni[3] Mrs. Pournima More[4] Harshal Indave[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]G. H. Raisoni College of Engineering & Management Pune, University of Savitribai Phule Pune Maharashtra, India

Abstract— Day by day, everyone is using internet all over the world. It is an ineluctable part of everyone's life. People are checking their personal e-mails, surfing over web, purchasing goods, playing online games, paying bills on the internet etc. However, while performing all these activities, how many people know about security? Do they know about risk of being attacked, infecting by malicious software? Despite some of the malicious software are spreading over network to create more threats by users. The behaviour analysis of client side cyber-attack play a significant role in computer security. In network surroundings find the activities that have an effect on Confidentiality, Integrity and accessibility on network knowledge. Currently, most computer systems use login IDs and passwords because the login patterns to verify users. However, many of us share their login patterns with co-workers and request these co-workers to help co-tasks, thereby creating the pattern united of the weakest points of computer security. In file integrity concept if any user deletes the file, modify file or insert file into specific directory then by using this system we can detect it. If any file delete, modify or insert into specific folder then that file backup will save in folder which is specified by client. Then file integrity log send to server. Server sends the integrity of that file to the clients E-mail. So client will easily know which file is modified, client can recover that modified file from specified backup folder. The aim of the system is analysing, understanding, watching and tracking hacker's behaviours in order to create more secure systems.

Keywords: IIDPS (Internal Intrusion Detection and Protection)

I. INTRODUCTION

In this system we work on network intrusion detection and to guard the network with the advent of snooping agents and honeypot on the network in order that any intrusion took place in network may be detected and as a result may be prevented. The snooping retailers and honeypot is used to provide network control in term of tracking. Usually in wireless networks, attacks are main cause of malfunctioning and are difficult to monitor. In file integrity concept if any user delete the file, modify file or insert file into specific directory then by using this system we can detect it. If any file delete or modify of insert into specific folder then that file will save in folder which the client specifies. Then file integrity log send to server. Server sends the integrity to the clients email id. So client will easily know which file is modified, client can recover that modified file from specified backup folder. In proposed system detecting the intrusion through many thing like DNS, IP, key log, integrity, checking currently running processes, etc. These all activities are performed by user. The first activity is file integrity. We are detecting intrusion through file integrity. If unauthorised person try to insert pen drive or access file then system send E-mail to user and shut down as the intrusion is detected.

II. PROPOSED SYSTEM

In proposed system, log file is stored into two different forms and in two different places. Log file in plain text is stored on target host and a copy of same log file is stored in another host called as log manager. When an intruder tries to change the log file on target host, this system running on the target host detects an intrusion and sends an alert e-mail/warning to the security administrator about it which in turn takes the required steps to mitigate it.

A. Methodology

1) Target Host:

Crucial data (i.e. log files, attacker image) is stored in the Target Host. The prime requirement to preserve the in-tegrity and confidentiality of the data stored in it is the continuous monitoring of the log file. And for this, our system is deployed on target host and it is continuously processed round the clock. Whenever an attacker tries to alter the target host, this system running on target host detects the intrusion; sends an alert e-mail/warning to se-curity centre as well as log server. At the same time, it invokes the digital forensic tool to capture the state of the system (RAM image and log file image). Newly captured log files image are compared with the previous data. And our Target Host is nothing but our Operating System as it is a Host based System. The intruder can access the system but if he tries to change any of the system properties and manipulate the records then the system comes into picture.

2) Server:

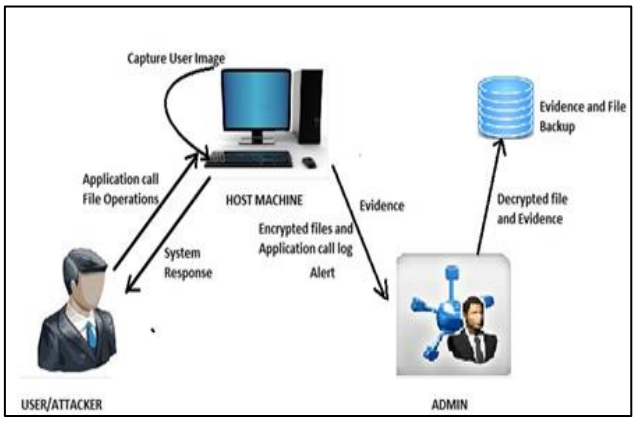
This server is used to store the copy of that particu-lar log file in a cryptographic format i.e encrypted form. Encryption key maintained only by the log server and it is kept personal. Periodically back up of that particular Target host log file is taken and after this encryption it is stored on the log server when the log file is received it encrypts the re-ceived log file and stores within it. The target host sends an alarm message to the log server, it will then decrypt the main login file, computes the im-age of the decrypted log file using DFT and trans-fer it to the target host to perform the comparison. If the intruder comes to know about the login sys-tem.then Key is the one which will protect the host machine.As the key will be available only with the owner.

3) Security Centre(Admin):

Security administrator uses this system to create an alert alarm using the Target Host. The Target host sends an alert E-mail to the security center and thus the job of the Security center starts. This attack is identifies and observed into the Security center. The security center is one of the most important function of this system when he/she tries to access this system and immediate alarm will be sent to the real owner. This will be done by the webcam recorder. When

he/she will turn off the internet connection and try to copy/paste data, immediately the PC will turn off within 10 seconds and webcam will capture the image of the intruder.

B. Proposed System



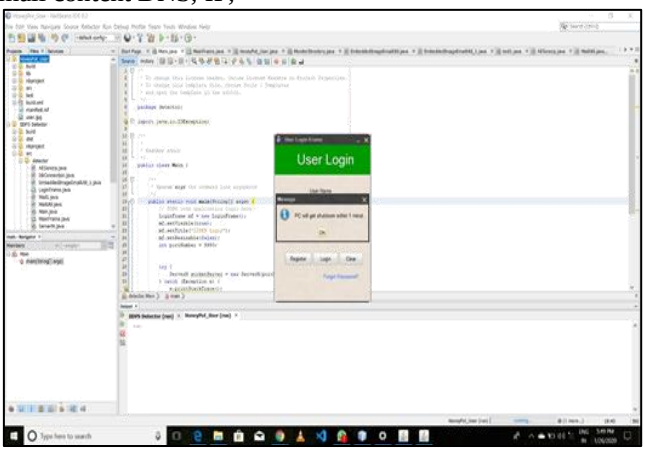
C. Implementation

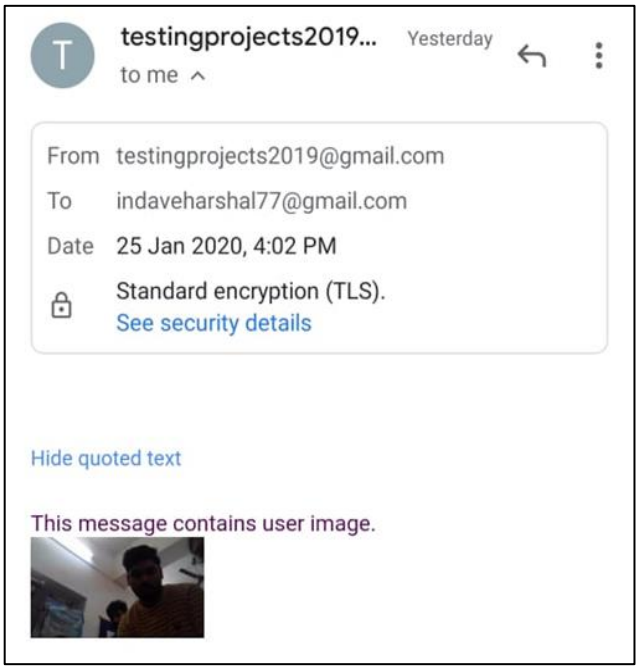
1) External Device Detection:
If User/Attacker try to connect external device to PC then Admin can receive alerts through email and capture the image of attacker.

2) Network Connection:
This system will check that is PC connected to active network or not, if PC is not connected to active network then pc will shut down at given specific time with alert of shutdown to user.

3) File Creation/Delete/Modify:
If attacker creates a new file, modify and delete then can receive alerts through email and capture the image of attacker.

4) Security Center:
Security admin get an alert alarm using Target Host. The Target Host sends an alert E-mail to security center. Alert E-mail content DNS, IP,





III. Conclusion and Future Work

When the habitual sc-pattern appears throughout the user's log file then it is counted, they usually used these patterns are removed out, and as a result user's profile is achieved. By inspecting the user's sc-patterns as his/her computer usage technique from the user's current input, this system resist terminated attackers. The experimental result that the percentage of average detection accuracy is very higher than 94%. When the decisive rate threshold is 0.9, indicating that this system can help system administration in insider attacker as well as outside attacker in throughout the attacking environment. The future study will be done by improving system performance and investigating third party shell commands

Acknowledgment

We take this opportunity to express my hearty thanks to all those who helped me in the completion of the Project on "Behaviour Analysis of Client Side Cyber Attack".

We would especially like to express my sincere gratitude to Prof. Pournima More, my Guide and Prof. Poonam Gupta HOD Department of Computer Engineering who extended their moral support, inspiring guidance and encouraging independence throughout this task.

We are also grateful to Dr. Vaibhav Hendre, Director of G. H. Raisoni College of Engineering And Management for his indis-pensable support, suggestions.

References

[1] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers Or how to thwart a phisher with trusted computing," in Proc. IEEE Int. Conf. Avail., Rel. Security , Vienna, Austria, Apr. 2007, pp. 120-127.

[2] C. Yue and H. Wang, "BogusBiter: A transparent protec-tion against phishing attacks," ACM Trans. Int. Technol. , vol. 10, no. 2, pp. 1-31, May 2010.

[3] Q. Chen, S. Abdelwahed, and A. Erradi, "A model-based approach to self-protection in computing system," in Proc. ACM Cloud Autonomic Comput. Conf. Miami, FL, USA, 2013, pp. 1–10.
[4] F. Y. Leu, M. C. Li, J. C. Lin, and C. T. Yang, "Detection workload in a dynamic grid-based intrusion detection environment," J. Parallel Distrib. Comput., vol. 68, no. 4, pp. 427-442, Apr. 2008.
[5] H. Lu, B. Zhao, X. Wang, and J. Su, "DiffSig: Resource differentiation based malware behavioral concise signature generation," Inf. Commun. Technol., vol. 7804, pp. 271-284, 2013.
[6] Z. Shan, X. Wang, T. Chiueh, and X. Meng, "Safe side effects commitment for OS-level virtualization," in Proc. ACM Int. Conf. Autonomic Comput. , Karlsruhe, Ger-many, 2011, pp. 111-120.
[7] M. K. Rogers and K. Seigfried, "The future of computer forensics: A needs analysis survey," Comput. Security, vol. 23, no. 1, pp.12-16, Feb. 2004.
[8] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting web based DDoS attack using MapReduce operations in cloud computing environment," J. Internet Serv. Inf. Se-curity , vol. 3, no. 3/4, pp. 28-37, Nov. 2013.
[9] Megha Mandlik, Trupti Akolkar ``Host Based Internal Intrusion Detection and Protection Techniques" Vol. 4, Issue 9, September 2016
[10] Jayesh Surana, Jagrati Sharma ``A Survey On Intrusion Detection System" 2017 IJEDR, Volume 5, Issue 2 ISSN: 2321-9939

