JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Automated Data Acquisition in SIEM for Incident Handling Process & Digital Forensics

[1*]Ritu Raj Gupta, [2]Ambreen Akhter, [3]Lalit Kumar, [4]Revathi T

[1*]Dep. of Information Technology, Jain University, Bengaluru, Karnataka-560069 India

[2]REVA Academy for Corporate Excellence, Bengaluru, Karnataka-560064 India

[3]Dep. of Information Technology, Jain University, Bengaluru, Karnataka-560069 India

[4]Dep. of Information Technology, Jain University, Bengaluru, Karnataka-560069 India

***Abstract*--** All associations ensure their data and information to direct their business effectively because as per the current situation where cyberattacks are increasing and data security is significant and everybody ensures safety. Digital Forensics has different stages Acquisition, Identification, Evaluation, and Reporting in which acquisition is a time-consuming process, and capturing the right information is always a challenging task. In real scenarios, due to the lag between detection of an issue and the acquisition of the evidence, forensics doesn't lead to effective analysis and conclusions. Digital forensics is not limited to a single operating system and it is already known different OS are deployed in a corporate environment. Each acquisition tool focuses only on one specific operating system, this usually means wasting time to find the right tool to acquire the right image at the time of the incident.

The purpose of this paper is to minimize the analysis time during an attack by acquiring only the required data in real-time without affecting the victim's machine during business hours and also transfer only the essential information for analysis that reduces network overheads, transfer time.

Keywords: *Digital Forensics, Operating system, Forensic investigation, Acquisition, Incident management.*

I. INTRODUCTION

Over the past several decades, emerging technological advancements created multitudinous opportunities for the miscreant to commit various crimes. The gradual increment in technology has dramatically changed the way of living life in the digital environment due to cybersecurity has become the latest trend. Cybersecurity is not just bounded to securing the critical information infrastructures but also in abundant fields like the IT industry, Cyberspace, government sector.

Advancement in cybersecurity will also increase protection, which includes the number of safeguarding solutions and one of the critical areas is to monitor all the infrastructure devices, logs in real-time that are managed by Security information and event management (SIEM) in an organization.

Once the incident gets trigged in the SIEM, the Incident management team will follow the structured approach that comprises various stages like identification, analysis, and recovery to make a routine service as soon as possible and to minimize the effect on corporate operations, preserving the highest levels of service quality.

Identification: It is the phase where incidents identify, logged, and categorized.
Analysis: It is the phase where the Analyst starts analysis and finds the root cause of the incident.
Recovery: It is the last phase of mitigation and patching of the incident take place.

The procedure for handling incidents is handled by the incident response team and forensic investigation team. For example, an intruder has gained unauthorized access to a computer system in an association Incident Response team would analyze the situation, determine the depth of compromise, and take corrective action.

The branch of forensic science like Digital forensic encompassing the data recovery and examination of evidence obtained on digital devices like computers, smartphones, hard drives, and other storage systems.

A computerized criminological examination has various stages: acquisition, preservation, analysis, and reporting. This paper is mainly focused on the Acquisition part of digital forensic investigation.

II. OBJECTIVES

The objective of this paper is achieved by implementing an automated script and capturing valuable information/data at the time of the incident without delay. The design is to decrease an opportunity to collect the information and make it productive. It captures the required information in real-time based on the incident without affecting user productivity.

The objective will be carried by following steps: -

1. SIEM will trigger an incident from the infected machine.
2. The infected machine's IP address will be captured by script.
3. SIEM will through the script for operating system checks, using Nmap like Windows, Linux, Mac, etc.
4. Based on the observation of OS results, a script will run to pull out active connections and running processes of the infected machine using SSH from a forensic machine.
5. Based on categories (OS-level, memory-level, network-level, and all) the required data will capture from an affected machine for further analysis that meets the requirement of specific incidents.
6. After capturing the required data, it will compress and generate hash values to maintain integrity.
7. The script will transfer the captured data to the forensic machine from the infected machine using SCP (secure control protocol).

III. METHODOLOGY

Acquisition of data is differently done than the traditional way of doing so. This is because SIEM is integrated with Infrastructure devices, affected machines, and code deployed on a Linux machine known as a forensic machine.

The implementation of this methodology follows the Incident handling approach differently and makes it efficient and has a collection of relevant data on which analysis to be performed to make better results in a minimal time. The purpose of this methodology is to minimize the adverse consequence of the incident by re-establishing ordinary help activity as fast as could be expected with automated scripts.

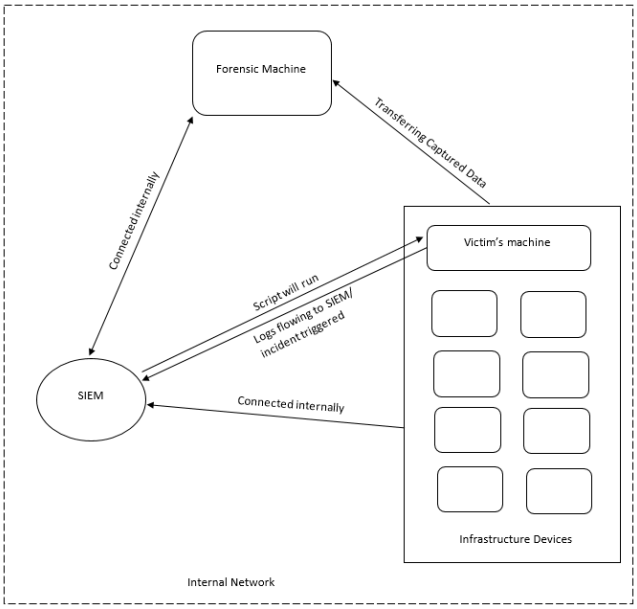
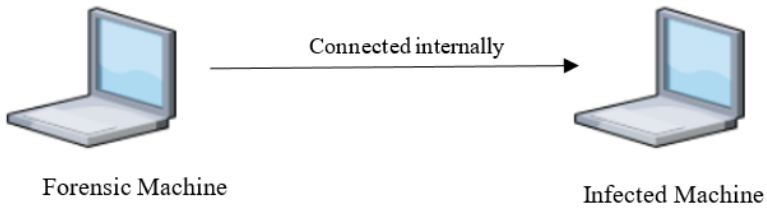


Fig.1.Methodology.

This approach can be carried out in an internal network of an organization where SIEM is integrated with all infrastructure devices and forensic machine that is deployed with an automated script. When SIEM will trigger an incident from an infected machine simultaneously script will run automatically to catch the necessary information from the infected machine and afterward move it to the forensic machine for examination.

IV. RESOURCE REQUIREMENTS

The asset prerequisite determination for this project. The figure shown below is the minimum setup required between the forensic and infected machine and the asset prerequisite for mechanizing the obtaining of the required information.



1. Linux OS
2. Nmap
3. OpenSSH server
4. OpenSSH client
5. Automated acquisition script

1. Any OS
2. OpenSSH server
3. OpenSSH client

Fig.2.Requirements.

V. SOFTWARE DESIGN

The software design is explained using the flowchart of automated script implemented to achieve the proposed output as shown below.

Start: SIEM will trigger an incident from the affected machine.
Captured IP: Script will capture the IP address of the affected machine.
Nmap: Script will run for operating system OS detection using Nmap command and provide the OS output of the machine related to a specific incident.

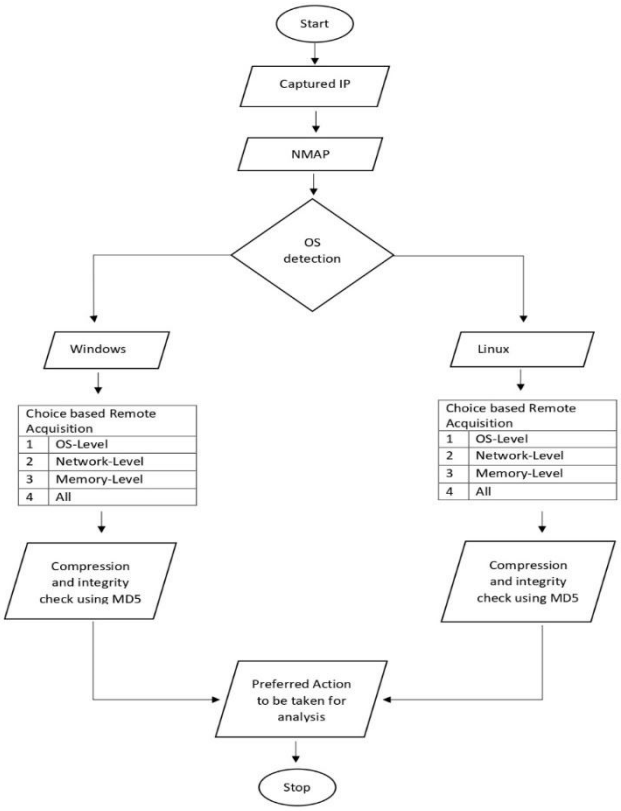


Fig.3.Software Design.

OS detection: Based on the observation of OS results script will run further steps like run a command to pull out active processes and running connections of the affected machine connected using SSH from a forensic machine.
Category list: Based on categories (OS-level, memory-level, network-level, and all) the required data will capture from an affected machine for further analysis that meets the requirement of specific incidents.
Compression: Once the required dump is received in the infected machine, the script will perform compression of capture data and transfer them to the forensic machine from the infected machine using SCP (secure control protocol).
Hash: Script will create a hash value of each file using MD5 hash after and before transferring the capture data to maintain integrity.

Analysis: SOC analyst will perform analysis on the capture data to find the root cause of the incident and mitigate it with the appropriate action.

VI. IMPLEMENTATION

The implementation of software design by preparing the automated script using the shell scripting programming concept, Nmap tool, SSH, MD5 hashes, SCP (Secure control protocol).

Note: Nmap is mandatory to be installed in a Forensic machine.

1. **OS detection:** Using Nmap script will run multiple checks on IP addresses to detect running operating systems on affected machines like Linux, Windows, and soon.
2. If Nmap detects the operating system as 'Linux/windows' an automated script will take root access (using SSH) of the affected machine and console the Active connections and Running processes in real-time.
3. For narrowing down our analysis script will pull out the dump as per our requirement from given categories for any detected operating system once SSH connection is made:

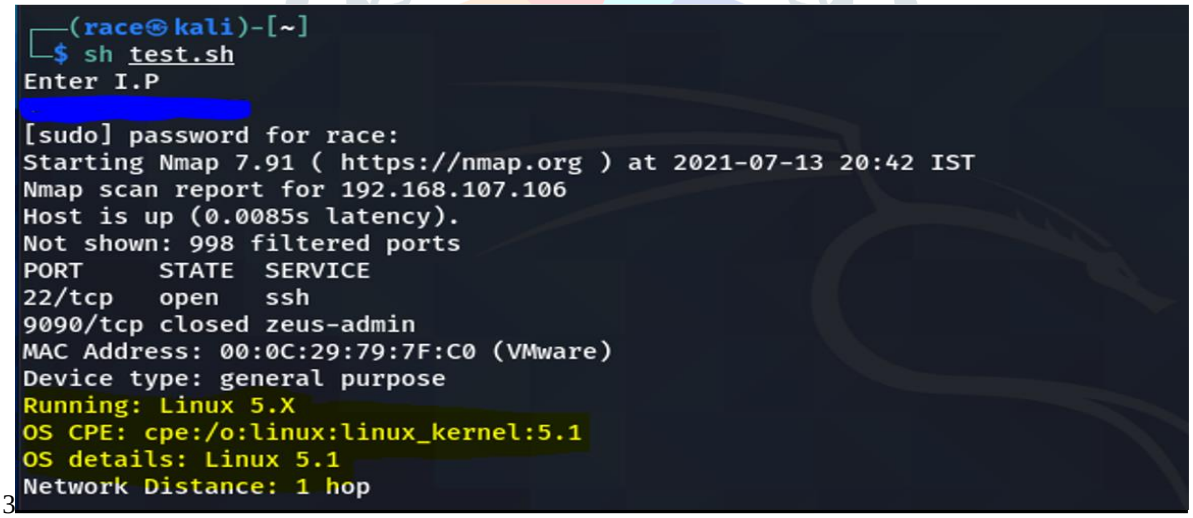
    - OS-level
    - network level.
    - memory-level.
    - All dump.

4. Based on our requirement script will hit the category list automatically and all related dumps files will be compressed and transferred to a forensic machine, after generating the MD5 hash value of each file to maintain integrity.
5. Once files are transferred to the forensic machine, the next step is to remove the same file from the affected machine.

VII. ANALYSIS AND RESULT

This part will explain the accuracy and quality of generated output through the automated script.
Below mentioned are the outcome at each step: -

1. **OS Detection result:** Script detected operating system as a Linux shown below.



3

Fig.4.OS Detection.

2. **Active Connection and Running Processes:** Using SSH pulled out the active connection and running processes of the infected machine.

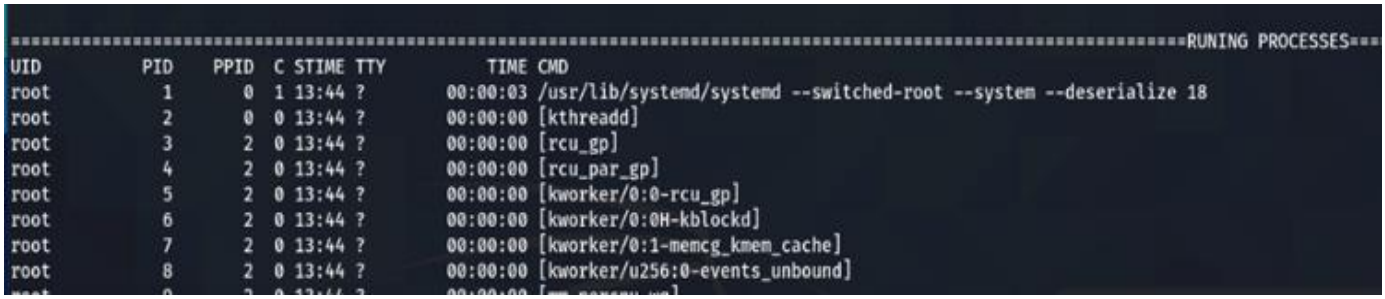


Fig.5.Running Process.

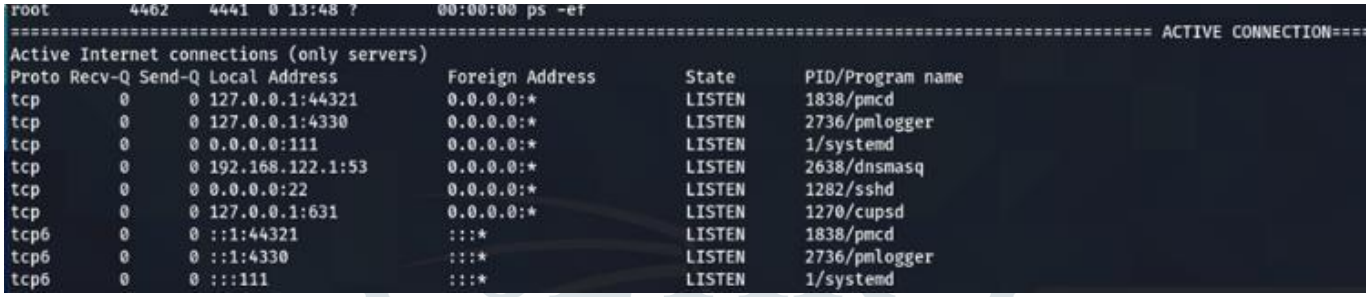


Fig.6. Active Connections.

3. **Category list:** Based on the defined incident, required data will get capture automatically once integrated with SIEM compress all the files and transfer them to the forensic machine from the affected machine using SCP (secure control protocol).

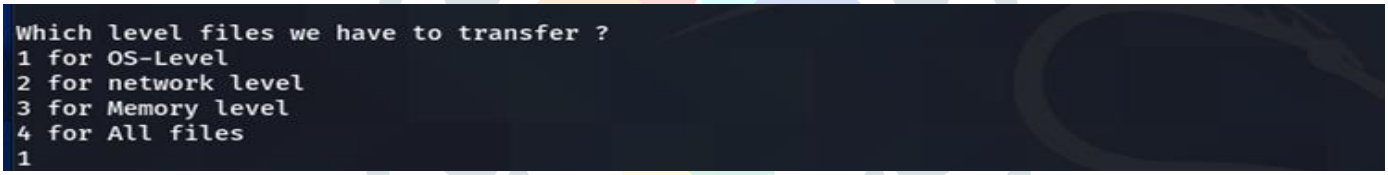


Fig.7. Category.

4. **Integrity check:** Script will generate the MD5 hash value of each file to maintain integrity.

Fig.8. Hash Value.

5. **Transfer:** All required data are transferred from the infected machine to the forensic machine successfully after compressing to make the best utilize of storage.

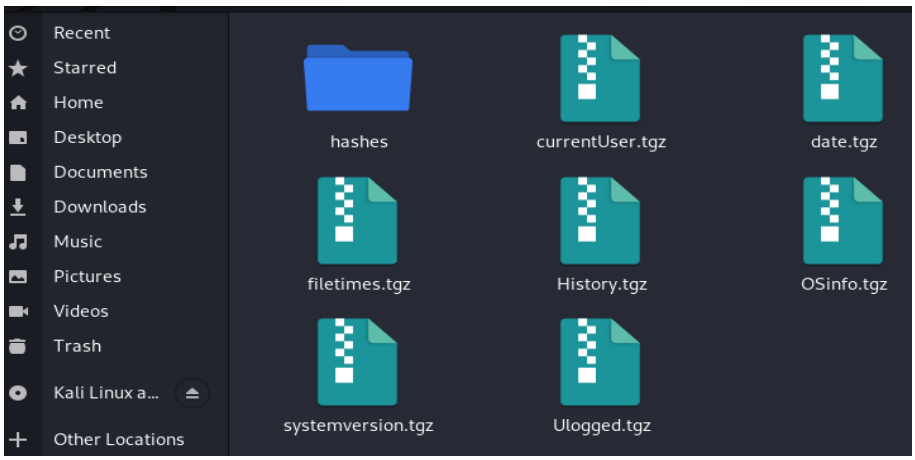


Fig.9. Data Transferred.

VIII. CONCLUSION

The conclusion of this project is to minimize the analysis time for the incident response and forensic investigation team by capture the required data related to the specific incident with the automated script. The potential use of this automated script will maintain the incident management phases from the time of the incident occurred till closure efficiently.

The implementation of this solution is cost-effective because the best option is to save the files on the local network from the affected machine. Storing the files in cloud storage directly from the evidence machine incurs the evidence destruction penalty of storing direct to disk, plus the overhead of storing, installing, and using the cloud storage software can be quite high.

This proposed solution scalability is, it can horizontally scalable, the script will run on a single machine and several machines simultaneously to capture the required data without effect.

The implementation of this project surely made it valuable to all cybersecurity organizations to develop new technologies and also prevent hackers/attackers in the reconnaissance stage only and save the infrastructure servers, devices, etc.

It can be improved later on the limitation of this project. For storage, an external memory drive is required to avoid crashing the system while performing the acquisition of heavy files.

Example: Sudo cat /proc/kcore>/root/AQUI/kcore

IX. FUTURE SCOPE

For future scope of work, improvement is to make separate categories for data extraction for all available use cases of security incidents in the implementation so that it will be easier to find the root cause of an incident/attack and this framework will save a lot of time.

This solution has good advantages but it will be more reliable if different APIs run all different steps in the script. In that case, the failure of one step will not affect the other step.

X. COMPLIANCE WITH ETHICAL STANDARD

This paper doesn't contain any research with human or animal subjects

XI. CONFLICT OF INTEREST

Ritu Raj declared that they have no conflict of interest.

XII. BIBLIOGRAPHY

[1] M. Scanlon and M. T. Kechadi, "Online acquisition of digital forensic evidence," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 31 LNICST, no. September, pp. 122–131, 2010, DOI: 10.1007/978-3-642-11534-9_12.

[2] F. Alrimawi, L. Pasquale, and B. Nuseibeh, "On the automated management of security incidents in smart spaces," *IEEE Access*, vol. 7, pp. 111513–111527, 2019, DOI: 10.1109/ACCESS.2019.2934221.

[3] C. Davis, *Hacking Exposed Computer Forensics, Second Edition*. 2009.

[4] V. Meera, M. M. Isaac, and C. Balan, "Forensic acquisition and analysis of VMware virtual machine artifacts," *Proc. - 2013 IEEE Int. Multi Conf. Autom. Comput. Control. Commun. Compress. Sensing, iMac4s 2013*, pp. 255–259, 2013, DOI: 10.1109/iMac4s.2013.6526418.

[5] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," *Proc. Digit. Forensic Res. Conf. DFRWS 2004 USA*, pp. 1–9, 2004.

[6] M. Kohn, J. H. P. Eloff, and M. S. Olivier, "Framework for a Digital Forensic Investigation," *Communications*, no. March, pp. 1–7, 2006, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.145.5855.

[7] J. Jones and L. Etzkorn, "Analysis of digital forensics live system acquisition methods to achieve optimal evidence preservation," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2016-July, pp. 0–5, 2016, DOI: 10.1109/SECON.2016.7506709.

XII. WEBILOGRAPHY

https://www.tecmint.com/ssh-passwordless-login-using-ssh-keygen-in-5-easy-steps/.
https://stackoverflow.com/questions/58222327/setting-up-password-free-ssh-from-linux-to-windows-10
https://superuser.com/questions/1319402/passwordless-ssh-from-linux-to-windows
https://github.com/lisandrogallo/simple-nmap-script/blob/master/simple-nmap-script.sh
https://blog.smallsec.ca/default-open-ports-in-windows/