International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

Analysis of Forensics Tools in Cloud Environment

Kajol Vilas Mohite[1], Prof. Varshapriya J. N[2]

[1]M.Tech Student, Dept. of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India
[2]Associate Professor, Dept. of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India

---

Abstract - Computer-forensic tool is been divided into various different parts like IoT forensic, digital forensic, network forensic and multimedia forensic. Cloud forensic is one of which is the combination of digital and network forensic. There are too many different tools creates for cloud forensic. This tools are the combination of digital and network forensic tool. Some tools uses base as mobile forensic detection and some of them uses base as network interface. Some of them are based on data extraction and other are based on image extraction from cloud database. In this paper we are testing different type of forensic tool and going to examine there performance on the different criteria. This criteria while help to understand the nature of forensic tool. How the tools detect the attacks on given cloud environment

***Key Words*: Cloud Computing, Cloud Forensic, Openstack, AWS, Security, Forensic Tool.**

1. INTRODUCTION

The Cloud has been a great influence on many applications by many different industries. With its popularity, cloud technologies are still problem understand and is open source for many research and development. The security of cloud computing is very critical topic which requires various additional research. From the forensic perspective, there are numerous questions which are arise like how to analyze the Cloud using traditional digital forensics techniques. For example, during a traditional digital forensic examination, all files that are storage in media are examined along with the overall file system structure. However, it cannot be considered as a practical model for cloud infrastructure, as the elasticity and ephemerality of pooled storage make pinpointing data blocks cumbersome. This difficulty is exacerbated in networked systems by the scale with which computing resources are spread over diverse administrative and geopolitical domains. Cloud is able to combine different heterogeneous resources (hardware platforms, storage back ends, file systems) that can be on geographically distributed.

Cloud Forensic Tool

1) EnCase: EnCase is normally used in criminal investigations and was named the Best Computer Forensic Solution for eight consecutive years by SC Magazine. There is no other solution which offers the same level of flexibility, functionality and can track the record of court-acceptance as EnCase Forensic. EnCase also offers mobile forensics, investigators finds the flexibility and convenience so that they can complete their investigations efficiently and quickly. Encase is also multipurpose forensic investigation tool.

2) FTK: FTK or Forensic toolkit is useful to scan the hard drive and looking for evidence. FTK is developed by Access Data and also has a standalone module called FTK Imager. It can be used to image the hard disk, ensuring the integrity of the data using hashing. It can image the hard disk in a single file for files in multiple sections, that are later joined and gets a reconstructed image as an output. Investigators can also choose between GUI or command line as per there convenience. FTK processes and indexes data upfront, which eliminates wasted time and waiting for searches to execute. Doesn't matter how many different data sources it is dealing with or the amount of data is to be cull through, FTK gets you there quicker and better than anything else. TK while computing uses distributed processing and it is the only forensics solution which provides fully leverage multi-thread/multi-core computers. Where other forensics tools waste all the potential of modern hardware solutions, FTK uses all 100 percent of its hardware resources, helping investigators find relevant evidence faster.

3) Oxygen Forensics: Oxygen Forensic Suite, it is used for gather digital evidence from cloud services used on phones and mobile phones. The suite is used to bypass the Android screen lock, and to get location history, extract data from cloud storages, analyze call and data records, search data keywords, recover deleted data and export data to various file formats. It supports various mobile platforms including Blackberry, Android, Sony, and iPhone.

2. RELATED WORK

There are some cloud forensic tools which were examined such as:

1) FROST: FROST provides the first forensic capabilities integrated with OpenStack, and to our knowledge the first to be a built into any Infrastructure-as-a-Service (IaaS) cloud platform. Throughout the a paper we use the NIST definition of cloud computing as a model for an on-demand access to a pool of resources that it can be as released with minimal management effort and

provisioned or a service provider interaction Consider an cloud customer, Alice, whose provider uses OpenStack with the FROST. Alice wants to an investigate an incident of suspiciously-high bandwidth usage from her cloud hosted webserver. While her a webserver logs web requests inside of its a VM, Alice can get am more complete pictures of a activity by obtaining an record of management activity and metadata about her VM. Alice uses FROST to retrieve firewall logs, Nova Compute Service API logs, and the virtual hard drive image of an suspicious machine and then provides this a evidence to the authorities. The firewall logs may also show a attacker scanning Alices virtual machine before hacking it. API logs may be contains evidence of unauthorized attempts to stop a virtual machine. The disk image may also contain evidence of what a attacker did once he obtained access. This is an strong forensic evidence about a potential crime that can be also used in court. Alice can also obtain this evidence by using either the an web management plane or the OpenStack API. FROST ensures that the forensic integrity of the an evidence that Alice gathers. Without FROST, the evidence would only be available with assistance from Alices cloud provider.

2) SIFT: SANS Investigation forensic toolkit is an VM that is a preloaded with the a tools required to perform forensic analysis. It is perfect for beginners, as it saves- tool finding, downloading and installation time. Based on Ubuntu, SIFT has all the important tools needed to carry out a detailed forensic analysis or incident response study. It supports analysis in advanced forensic format (AFF), expert witness format (E01) and RAW evidence (DD) format. It comes with tools to carve data files, generate timeline from system logs, examine recycle bins, and much more. SIFT provides user documentation that allows you to get accustomed to the available tools and their usage. It also explains where evidence can be found on a system. Tools can be opened manually from the terminal window or with the help of top menu bar.

3. PROPOSED METHOD

AWS-IR

It is an Python command line interface that is automates initial response actions. It has two built-in commands, key-compromise and instance-compromise, with some plugin options. As the name implies, key-compromise disables and revokes compromised access keys for you. Instance-compromise isolates the occurrences and preserves forensic artifacts for your investigation.

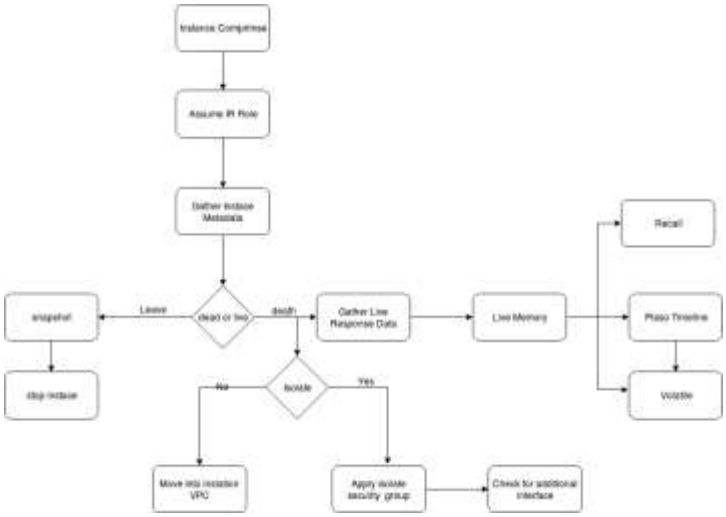

Fig -1: Flow Diagram on AWS

Margarita Shotgun

This is another Python command line tool, but this one allows you to pull memory from one or more systems in your AWS environment.

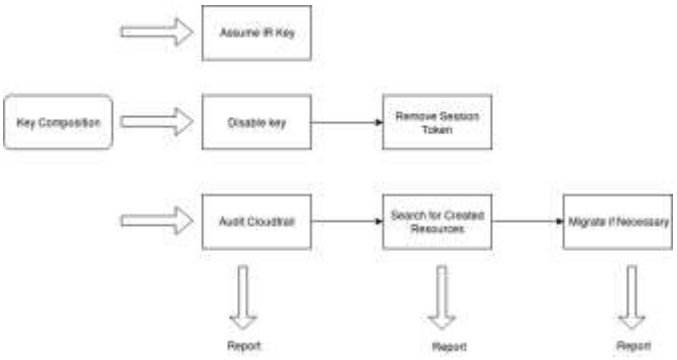

Fig -2: Key Examination

4. EXPERIMENT, EVALUATION AND DISCUSSION

4.1 Algorithm and Cammands

Installation of AWS

$ sudo apt _get update

$ sudo apt _get upgrade

$ sudo apt _get install python –pip

$ python3 –m virtualenv env

$ source/env/bin/activate

$ pip install aws ir

Installation of Margarita

$ git clone https://github.com

/ThreatResponse/margaritashotgun.git

$ cd margaritashotgun

$ python setup.py sdist

$ pip install dist/margaritashotgun−*.tar.gz

$ margaritashotgun−h

Small Phase of work flow of the tool

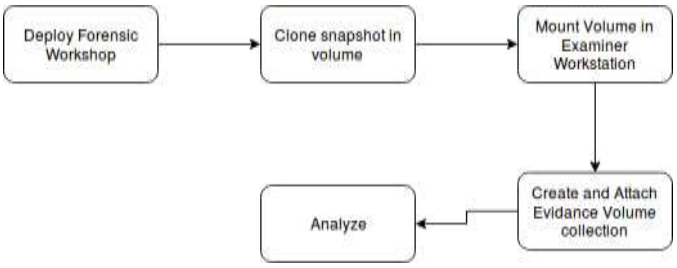

Fig -3: Flow of how snapshot is analize

4.2 Factors that lead to test performance:

There are several opportunities that can be leveraged to advance forensic investigations.

• Cost Effectiveness: It is secure and the forensic services can be less expensive when they are implemented on a large scale. Cloud computing is very attractive to small and medium enterprises because it helps in reducing IT costs.

• Data Abundance: Amazon S3 and Amazon Simple DB ensure object durability by storing objects multiple times in multiple availability zones on the initial write.

• Overall Robustness: Some technologies help improve the overall robustness of cloud forensics. For example, Amazon S3 automatically generates an MD5 hash when an object is stored

• Scalability and Flexibility: Cloud computing facilitates the very flexible and scalable use of resources, which also applies to forensic services.

• Forensics as a Service: Forensics as a cloud service could be leverage the a massive computing power of the cloud to support cybercrime investigations at all levels

5. CONCLUSION

This paper shows how to the study of latest forensic tool used by AWS services. And there architecture that how it takes snapshot of every instance and verifies whether it is safe or not. The given tool is just simply taking the snapshotof every instance also. There are many old cloud forensic tool which are used which uses encrypted data for analyzing the system. It uses can be run on hardware as well as on instances or on built in cloud environment. But the given tools which this paper is working on is been provided by Amazon Web Services and are more secure that other forensic tool.

REFERENCES

[1] Sameera Almulla, Youssef Iraqi,Andrew Jones , "Digital Forensic of a Cloud Based Snapshot," IEEE Transl., 978-1-5090-2000-3, The Sixthen Intenation Conference on Innovating Computer Technology, INTECH 2016.

[2] Aincent E. Urias, William M.S. Stout, Caleb Loverro, Hypervisor Assisted Forensics and Incident Response in the Cloud, SAND 2016eng Guo, "An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing", IEEE transaction on cloud computing May, 2016.

[3] Pragya Jain, Aparna Datt, S.C. Gupta, "Cloud Service Orchestration based Architecture of OpenStack Nova and Swift ", Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016

[4] Amna Eleyan,Derar Eleyan, "Forensic Process as a Service (FPaaS) for Cloud Computing," IEEET Transl, European Intelligence and Security Informatics Conference, IEEE, 2015.

[5] Monali P. Mohite, S. B. Ardhapurkar , "Overcast: Developing Digital Forensic Tool in Cloud Computing Environment," 978-1-4799-6818- 3, IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems, ICIIECS'2015.

[6] Josiah Dykstra*, Alan T. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform,"www.elsevier.com/locate/diin, 10 (2013) S87S9.

[7] Filipo Sharevski, "Digital Forensic Investigation in Cloud Computing Environment: Impact on Privacy," 978-1-4799-4061-5, IEEE Louisville Chapter,2013 IEEE

[8] "Amazon Web Services. Amazon CloudWatch" http://aws. Amazon.com/cloudwatch/;, 2013

[9] K.K. Arthur H.S. Venter, "An Investigation into Computer Forensic Tools," Information and Computer Security Architectures (ICSA) Research Group, 2013

[10] Anand Kumar Mishra, Priya Matta, Emmanuel S. Pilli and R. C. Joshi, " Cloud Forensics: State-of-the-Art and Reasearch Challenges, International Symposium on Cloud and Services Computing 2012

[11] K, Ruan, J. Carthy, T. Kechadi and M. Crosbie, "Cloud Forensics," Advances in Digital Forensics VII - IFIP Advances in Information and Communication Technology, Volume 361, pp. 35-46, 2011

[12] Monali P.Mahiteand,Pallavi R.Gulve, " Quantitative Analysis of Cloud Based Digital Forensic Tool,"., 2009.