Supplementing Live Forensics with Traditional Forensics for Cloud Computing

Mohammed Younus Siddiqui, Faizuddin Mohammad, Ahmad Almulhem

King Fahd University for Petroleum and Minerals,
Dhahran, Saudi Arabia.

The 26th Annual IEEE Software Technology Conference (STC2014)
29 March - 3 April 2014

Outline

- INTRODUCTION
- MOTIVATION
- LIVE FORENSICS
- RELATED WORK
- LIVE FORENSIC INVESTIGATION
- TRADITIONAL FORENSIC INVESTIGATION
- FUTURE WORK
- CONCLUSION

introduction

- Digital forensics is fast becoming an important field as more and more criminals use technology for their illegal activities.

- ”Digital forensics encompasses approaches and techniques for gathering and analyzing traces of human and computer-generated activity in such a way that it is suitable in a court of law.”
  - Stephen Wolthusen

introduction

- Digital forensics process
- • Collection: This is the first phase in forensic process where the acquired data is identified, labelled and recorded.
- • Examination: The collected data must be forensically processed either manually or automatically.
- • Analysis: The results obtained from the examination stage should be analyzed using legally justifiable techniques and methods.
- • Reporting: The results of the analysis should be reported in a clear and understandable manner.

introduction

- The success of cloud computing has brought unwanted attention from criminals.

- It could be used a tool as well as a target for malicious activities.

- As such, there is an urgent need of digital forensics techniques that can be applied to the cloud.

motivation

- To aid investigators when they come across a cloud which is being used for criminal purposes.
- Such a cloud could be a private cloud owned by the criminal or a public cloud having the criminal as one of its many users.
- As such, the cloud cannot be shut down as doing so would either result in loss of crucial evidence or loss of service to other legitimate users.
- Live Forensics remains then the only viable option.

LIVE FORENSICS

- Live forensics is the analysis of the system while it is still running.
- A lot of information can be recovered while the system is running which would have not been available otherwise.
- Live forensics becomes all the more important and necessary when a cloud must be kept running is involved.
- Moreover, due to the large amounts of data in the cloud, it becomes all the more difficult to apply traditional forensics to the cloud.

Related Work

- Birk and Wegner [3] present few potential sources for finding data in the cloud for forensics. The potential sources for evidential data are the virtual cloud instances); network layer and client system.
- Taylor et al. [4] examines legal aspects of the digital forensic investigation of cloud computing and in particularly focuses on the UK legal system.
- Maritni and Choo [6] proposed an integrated iterative framework based upon the two widely used digital forensic frameworks of Mckemmish and NIST which can be used to perform digital forensic investigation in the cloud computing environment.

Related work

- Delport et al. [8] propose isolating a cloud instance for performing a digital forensic investigation. They propose seven techniques i.e. Instance Relocation, Server Farming, Failover, Address Relocation, Sandboxing, Man in the Middle and Lets Hope for the Best.
- Zafarullah et al. [9] suggest that the operating system and security tools present inside the cloud should implement logging because digital forensics mainly relies on analysis of logs for identifying suspects.
- Dykstra and Sherman [10] focus on applying digital forensics to IaaS cloud computing technology. They discuss the technical and trust issues associated with such a cloud model.

Live forensic investigation

- Evidence Source Identification and Preservation:
  - Live Forensics is performed on the CloudStack cloud while the attack is in progress.
  - The CPU usage of the Management Server at the time of attack has risen to 95.5 percent.
  - At normal conditions, the usage is very low.
  - By monitoring the abrupt change We first identify the potential sources of evidences in the Management Server and then perform data gathering.

Live forensic investigation

- COLLECTION:
  - Netcat program [15] was used to collect the information that was identified during the live forensic investigation.
  - It is a network utility which uses the TCP/IP protocol to read and write data across network connections.
  - We used another VM as the remote host to store the data from live forensics.
  - The table shows the type of data collected and the corresponding general Linux commands which was run to obtain that particular data.

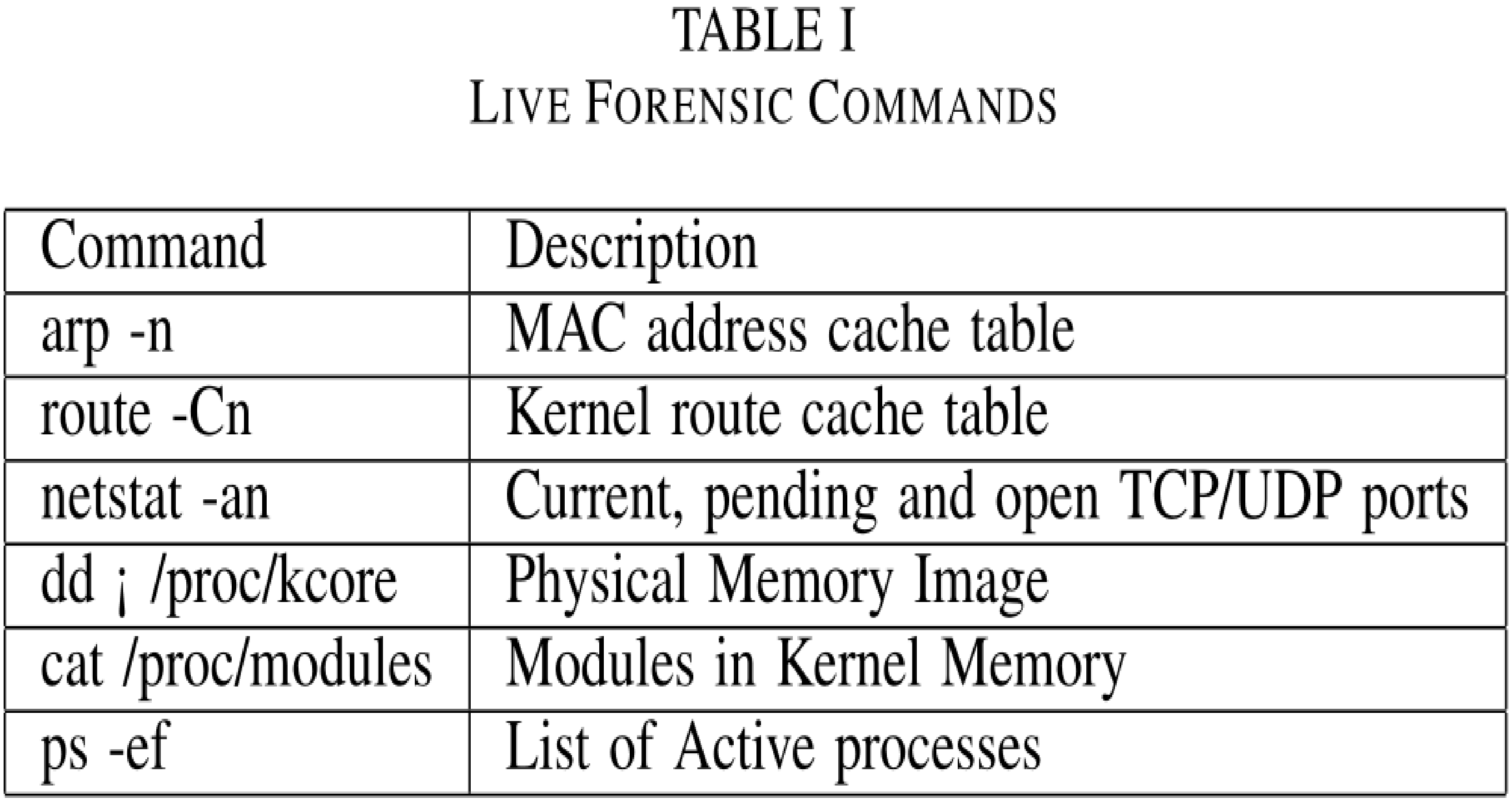

TABLE I

LIVE FORENSIC COMMANDS

Command	Description
arp -n	MAC address cache table
route -Cn	Kernel route cache table
netstat -an	Current, pending and open TCP/UDP ports
dd ¡ /proc/kcore	Physical Memory Image
cat /proc/modules	Modules in Kernel Memory
ps -ef	List of Active processes

Live forensic commands

LIVE forensics investigation

- Examination and Analysis:
- MAC Address Cache Table:
  - List of IPs of the machines connected to the network and their corresponding MAC addresses was obtained.
  - The IP address of the machine used to perform DoS was among the list. It is shown in figure.

Live forensic investigation

- Examination and Analysis:
- Kernel route cache table:
  - The routing table was obtained.
  - This contained the list of routes between gateways and hosts as shown in figure.

Live forensic investigation

- Examination and Analysis:
- Current, pending connections and open TCP/UDP ports:
  - The list of TCP connections, ports used and their state was recorded that can be seen in the Figure 7.
  - The list contained a high number of tcp connections at port 8080 in the WAIT state.
  - This showed that a DoS using TCP connections was being performed at port 8080.

Live forensic investigation

- Examination and Analysis:
- Running processes:
  - The list of active processes was recorded. By analyzing this data, any suspicious process can be detected.
  - In our data, we were able to find HeapDumpOnOut-OfMemoryError for the cloud management process as shown in Figure.
  - This showed that the DoS attack was successful.

Traditional Forensic Investigation

- Traditional forensics was performed on CloudStack once the attack had finished.
- Traditional forensics is also known as dead forensics as it is done on a system that is not running.
- Traditional forensics was performed to supplement the evidence obtained during live forensic of the cloud.
- The integrated conceptual digital forensic framework for forensic is followed in order to get the best results.

Traditional Forensic Investigation

- Evidence Source Identification and Preservation:
  - The management server was the target of the attack; hence it becomes the primary source of evidence for our traditional forensic investigation.
  - The files present in the management server are identified as the main source of information.
- Collection:
  - The image of the hard disk drive was obtained using FTK imager [16].
  - FTK imager is a disk imaging program provided for free by AccessData which is used to make perfect copies of the data without making changes to the original evidence.

Traditional Forensic Investigation

- Examination and Analysis:
- FTK imager was used to analyze the disk image obtained during traditional forensic investigation.
- The disk image was the copy of the Management Server’s hard disk.
- FTK imager was able to display the files and folders inside the disk image.
- From live forensic investigation, we came to the conclusion that a DoS attack was being performed to the Management Server’s UI.
- By analyzing the logs in the disk image as shown in Figure, we can confirm that the UI was really the target of the attack

Traditional Forensic Investigation

- Reporting and Presentation:
- On close examination of the access logs, we observed that a huge number of hits to the UI were coming from IP address 192.168.0.5.
- This confirmed the findings of the live forensic investigation.
- Thus, we were able to supplement live forensic investigation with traditional forensic investigation in a cloud computing environment.

Future work

- In future, a real test bed can be setup by acquiring more resources.
- We intend to perform the same experiment for the VMs hosted in the cloud infrastructure.
- VM introspection will be used on the XenServer as it is a powerful forensic tool.
- Commercial forensic tools can be used and their applicability in digital forensics can be tested in the future.

Conclusion

- We discussed Traditional and Live Digital Forensics and applied these forensic techniques to an open source cloud, i.e., CloudStack.
- We launched an Http DoS attack on the cloud and performed the forensics with open source tools.
- The result obtained from the live forensics is supplemented with that of the traditional forensics.
- By doing so, we were able to obtain substantial evidence about the type of attack, the target IP and port of the attack, and the IP of the attacker.
- This demonstrated the capability of general open source tools for performing digital forensics on a cloud computing platform.

ANY Questions?

Thank you for listening.