NMBaaS (Non-Malicious Botnet as a service): Achieving Digital forensic Readiness in a private cloud using NMBaaS

COS301-PROPOSAL

1. Introduction
The pervasiveness of the Internet, increased number of devices and the dissemination of ICT have played a big role in the increase in number of security incidents and adversaries in the cloud. However, there are limited proactive strategies that can enable mitigation of these incidents given the distributed nature of cloud resources. Therefore, the primary aim of the work described in this proposal is to investigate and propose a contribution on how Digital Evidence can proactively be acquired from the cloud environment for purposes of Digital Forensic Readiness using a robot network in a non-malicious fashion [1]. Digital forensic readiness minimizes the cost of performing a digital forensic investigation [5].

2. Problem statement
Corporate investigation teams and law enforcement agencies face unrelenting task in trying to proof that an electronic event has occurred in the cloud environment. Due to this, a number of digital forensic investigators have tried to proof the existence of digital evidence in the cloud infrastructure but getting log information is a challenge because logs are decentralized across several and multiple servers [4]. However, there does not exist any easy way of conducting digital forensic readiness in the cloud architecture without modifying the cloud architectures. A botnets should therefore have the capability of forensically harvesting potential digital evidence and digitally preserving it.

3. Project Visions and Objectives

3.1. Visions

1. To provide users with an insight on the performance of cloud computing from a digital forensic perspectives.
2. To align the users on the benefits of organizational forensic readiness and the cost-effectiveness.
3. To improve proactive digital evidence management techniques in the cloud environment, through improved ways of retaining potential digital evidence.
4. To improve the organization’s response to incidents, and threats in the cloud environment by providing a timeous forensic response.

3.2. Objective

The objective of NMBaaS is to build an application prototype that shows how digital data that can be used for digital forensic readiness purposes can forensically be captured in the cloud environment through scientifically proven digital forensic processes. In solving this problem, a Non-Malicious Botnet (NMBaaS) that is able to capture digital data for digital forensic readiness purposes is deployed in the cloud. The application to be developed shall cut down the cost of performing a digital forensic investigation. Primarily the focus of the NMBaaS is to develop a system that is able to capture information in a virtual environment without modifying the architecture.

4. Project owner

University of Pretoria

5. Scope of the project

This project will consist of development of a prototype that proves that historically a malicious botnet can be modified and used as a service when it operated in a non-malicious fashion. This can be done by creating infection vectors in a virtual environment using the NMBaaS that are able to capture potential digital evidence in the cloud environment without need of modifying the hypervisor or the existing architecture of the cloud. The botnet should be able to capture, hash and preserve digital data that can be used for digital forensic readiness purposes. Further the captured digital data can be used to support or refute a hypothesis in a court of law which would otherwise not be possible. The following shows the use-cases and functional requirements needed for the (NMBaaS) project.
The underlying assumption in this project is that $N$ numbers of virtual machines within a given cloud are being provided services by the Cloud service providers (CSPs). Sensitive and critical information can be gathered in a non-malicious fashion from the cloud through the bots installed in the $N$ number of virtual machines.

In this project “Infection” carries a positive connotation where the vectors of the NMBaaS are able to run in virtual instances and be able to capture digital information in the cloud environment. Infection in this context involves injecting code in the cloud that can extract digital information. The captured digital data from the cloud environment should be used in preparing for digital forensic readiness as potential digital evidence if an incident is detected in the cloud.

2. **Forensic Administrator**

The forensic administrator ensures that digital data is captured in a logging process as shown in the use-case in figure 1. During preservation, the integrity of the collected data is maintained by means of log hashing before it is exposed to DF investigators and law enforcement agencies. Hashing is performed as a block of hashes to potential evidence to maintain the integrity of the data. A comparison of cryptographic hash functions is performed on the logged data to ensure that its integrity is maintained. The significance of digital information preservation is to ensure changes are not made to the gathered potential evidence. PDE to be used for DF readiness has to be retained in its original form.
3. Law enforcement

In this context, pre-incident detection is used as a process that prepares possible potential evidence to be used for DF investigation. On the other hand, pre-incident analysis is a process of extracting exact evidence that may be admissible in a court of law. During pre-incident analysis, the originality of potential evidence is proved by comparing the hash of the preserved data.

Forensic reporting is a crucial stage during which a DF evidence examiner needs to recognise a roadmap of the steps undertaken during the proactive process before evidence is considered as admissible. This is the final stage and whatever is provided in this case has to be used by DF investigators and law enforcement agencies.

6. Architectural requirements

The following are the quality attributes that the NMBaaS system needs in order for it to achieve its roles.

6.1. Quality Requirements

- Security
- Usability
- Reliability
- Maintainability
- Administability

3.1 Basic Operation of the NMBaaS

The architecture in figure 2 considers the cloud environment, which consists of CSPs and the NMBaaS. The CSPs provide virtual services to cloud users whereas the NMBaaS is implemented as a (SaaS) delivery model. This is shown by the arrow pointing from the CSPs to NMBaaS box labelled 1. The NMBaaS ‘infects’ the virtual instances of the users as a service within a network in the next step.
In the step labelled 2, the system encompasses N number of virtual machines. In this step the NMBaaS ‘infects’ the virtual machines with bot clients, as is shown by the arrows pointing inside the VMs. Thereafter, in the step labelled 3, the bot clients proactively capture distributed acute traffic in the cloud that moves as possible attack logs in the logging process. The bot clients are able to gather both non-volatile and volatile digital data from target VMs and from the network in the cloud. The captured logs are categorised as monitored data, service artifacts and forensic logs. All the captured logs are sent to a centralised digital preservation centre for log management in the next step.

In the step labelled 4 (with the arrows pointing downwards), the captured potential evidence in the form of logs is hashed before being preserved digitally. Hashing is performed as a block of hashes to
potential evidence to maintain the integrity of the data, as shown, using block 1, block 2….block n. In this context, a block is a set of captured logs. A comparison of cryptographic hash functions is performed on the logged data to ensure that its integrity is maintained. The significance of digital information preservation is to ensure changes are not made to the gathered potential evidence. PDE to be used for DF readiness has to be retained in its original form.

This is followed by the step labelled 5. In this context, pre-incident detection is used as a process that prepares possible potential evidence to be used for DF investigation. On the other hand, pre-incident analysis is a process of extracting exact evidence that may be admissible in a court of law. During pre-incident analysis, the originality of potential evidence is proved by comparing the hash of the preserved data. This is shown using two-sided arrows pointing to the part labelled step 5.

The step labelled 6 shows the reconstruction of forensic events. Reconstruction shows how the events occurred. This is achieved through taking the timestamps of collected potential evidence and checking the pattern of occurrence. This is shown by the arrow labelled no 6

The final part of the system is the forensic reporting phase. This has been shown by the part labelled 7 with an arrow pointing downwards. Forensic reporting is a crucial stage during which a DF evidence examiner needs to recognise a roadmap of the steps undertaken during the proactive process before evidence is considered as admissible. This is the final stage and whatever is provided in this case has to be used by DF investigators and law enforcement agencies. This is shown with the arrow labelled 7.

7. Skills

The preferred skills is C++ but it is not limited to any other subject to discussion.

8. Deliverables

The following are the deliverables that will be expected at the completion of the project.

1. Source code
2. Code for testing.
3. Documents
   - Requirements
   - Architecture
   - Test plans
   - Design
   - User’s manual
   - Installation manual
4. Build and deployment scripts
5. Issues report

References:


