# Chapter 70
# Hack the Cloud:
## Ethical Hacking and Cloud Forensics

**Mark Crosbie**
*IBM, Ireland*

## ABSTRACT

*The goal of this chapter is to explain the challenges that the forensic investigator faces when investigating Cloud Crime and how they can learn from the techniques used by Ethical Hackers to improve their investigation technique. The security threat posed by hackers on the Internet is constantly evolving. Cloud computing provides new avenues for hackers to exploit organizations, giving rise to new classes of vulnerability, and new security challenges. The forensic investigator must learn to "think like a hacker" so that they can reconstruct the path the hacker takes through the cloud environment. This chapter will explain how an Ethical Hacker works, how the Ethical Hacker views the Cloud, and in doing so illustrate the new challenges facing a forensic investigator.*

## INTRODUCTION

The security threat posed by hackers on the Internet is constantly evolving. As security professionals improve the defensive posture of systems and networks, hackers have evolved their penetration techniques. Moreover, the nature of the attacks launched against the Cloud is changing. The rise of Web applications and Web services has provided a common foundation for hackers to exploit, independent of the underlying operating system or software stack. In the past hackers would have focused on system level exploits, requiring them to research, develop, and test a malware exploit that was fine-tuned for a particular operating system platform and version. Web application vulnerabilities are platform-neutral, and can be exploited using text-based scripting languages such as JavaScript.

As defined in Kent et al. (2006), digital forensics focuses on recovering electronic evidence for presentation in a court of law. The job of the forensic investigator is to reconstruct the activities of the hacker after-the-fact. Grobauer and Schreck (2010) identified the following forensic challenges within the cloud computing environment:

- Separation of customer's data sources during evidence collection.
- Adapting forensic analysis methods to the Cloud.
- Improving live analysis techniques.

DOI: 10.4018/978-1-4666-6539-2.ch070

- Improving log generation and analysis techniques.

Hackers and criminals are aware that the forensic investigator will face these challenges, and will adapt their attack techniques to leverage the four challenges identified above. The remainder of this chapter explains how a hacker will target a Cloud with a view to committing a crime, and how they will use the very aspects of the Cloud that make it appealing to businesses against the forensic investigator.

The forensic investigator must have an awareness of the types of crimes possible in the Cloud. There are two scenarios to consider:

1. The Cloud is the target of the crime, and the likely victims of the crime are clients of a cloud provider.
2. The Cloud enables the crime to be committed, by providing services that would be otherwise unavailable to the criminals.

## THE CLOUD AS THE TARGET

Enterprises who adopt cloud-computing models hope to see their costs reduced as applications and services, which were once provided in-house, are moved to a shared infrastructure. By outsourcing the provisioning and maintenance of hardware, software and applications they hope to see cost reduction while increasing their ability to rapidly deliver service. However, the cloud computing model also offers hackers a unique advantage; a concentration of valuable targets are one present on a single shared infrastructure model. Vulnerabilities in the underlying cloud provider infrastructure will likely compromise every customer resident in the Cloud.

Cloud computing is deployed in one of three service models. Mell and Grance (2011) have defined the three service models as Software as a Serivce (SaaS), Platform as a Serivce (PaaS) and Infrastructure as a Service (IaaS). By understanding how the hackers target the cloud service models the forensic investigator can prioritize how they gather data needed to prosecute the crime. For each service model, a hacker will target the underlying cloud infrastructure used to provision the applications. The cloud provider must provide functions to customers to manage the instances of the running applications they purchase. For example, a cloud provider may provide functions to add users into the services (termed on-boarding), delete dormant user accounts, and view user activity. If an attacker can compromise the cloud provider functions to manage the application they can gain access to the customer's data by adding themselves as a legitimate user (or administrator) of the application.

### Software as a Service (SaaS)

In the Software as a Service model, the cloud provider is providing a hosted instance of an application. For example, a hosted email service offered by a SaaS cloud provider would provide a fully functional email application instance for customers to begin loading data into. Customers in the cloud provider do not have access to the underlying software stack, operating system, and hardware (nor do they wish to). The cloud provider is trusted by the customers to maintain the security and availability of the application to an agreed service level.

Typically, applications in a SaaS environment are Web applications. Web applications have a long history of known security flaws. The hacker can launch attacks against the application used by a customer and attempt to subvert the security of the application. This attack vector may also give the hacker access to data stored in the cloud provider belonging to other customers.