IDEA GROUP PUBLISHING **ITB13034**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter I

An Overview of Electronic Attacks

Thomas M. Chen, Southern Methodist University, USA

Chris Davis, Texas Instruments, USA

Abstract

This chapter gives an overview of the major types of electronic attacks encountered today and likely to continue into the foreseeable future. A comprehensive understanding of attackers, their motives, and their methods is a prerequisite for digital crime investigation. The range of possible cyber attacks is almost unlimited, but many attacks generally follow the basic steps of reconnaissance, gaining access, and cover-up. We highlight common methods and tools used by attackers in each step. In addition, attacks are not necessarily directed toward specific targets. Viruses, worms, and spam are examples of large-scale attacks directed at compromising as many systems as possible.

Introduction

Today computer systems are often invaluable for business and personal uses. Computer systems store valuable corporate and personal information while computer networks provide convenient data access and processing services. They are naturally very tempting targets, as shown by statistics that track the frequency and prevalence of cybercrimes. For example, an CSI/FBI survey found that 71% of organizations had experienced at least one attack in 2004, while the remaining organizations did not know the number of attacks (Gordon, 2005).

The ease of carrying out electronic attacks adds to the temptation for attackers. It is widely known that computer systems have numerous vulnerabilities, although not every attack exploits vulnerabilities (Hoglund & McGraw, 2004). In the second half of 2004, 54 new vulnerabilities per week were discovered on average, and 50% were serious enough to be rated as highly severe, meaning that exploitation of the vulnerability could lead to complete compromise of a system (Turner, 2005). Attackers are keenly aware of new vulnerabilities because it takes time for organizations to set up adequate protection. New vulnerabilities are announced along with a software patch, but organizations are sometimes slow to apply patches. In late 2004, exploit codes for new vulnerabilities appeared on average only 6.4 days after the announcement of the vulnerability; in early 2004, it was 5.8 days. Organizations that are slow to patch are often vulnerable to new exploits.

Attackers are also well aware that virtually all computers are interconnected by the Internet or private networks. Moreover, mobile and handheld devices with Internet connectivity have steadily grown in popularity. Networks make attacks easier to carry out remotely and more difficult to track to their sources.

This chapter gives an overview of electronic attacks, organized according to the basic steps of reconnaissance, gaining access, and cover-up. We focus here on network-enabled attacks, but this is not meant to imply that all electronic attacks are carried out remotely. Direct physical attacks on computers are also quite common but not covered here. This chapter also describes large-scale attacks such as viruses, worms, denial of service, and spam. An understanding of attackers and their attack methods is a prerequisite to digital forensics, which is concerned with the collection and analysis of evidence of electronic crimes. This chapter serves as necessary background for other chapters in this book that cover aspects of digital forensics in depth.

Types of Attackers and Motives

As one might expect, there are as many different types of attackers as there are different types of attacks. Attackers can be categorized in a number of different ways. For example, attackers may be either internal or external, depending on their relationship to the target. In the past five years, the fraction of attacks from inside have been roughly equal to the fraction from outside (Gordon, 2005). Insiders are worrisome because they have certain advantages such as trust and knowledge of the target organization that can increase the chances of a successful attack. Moreover, insiders do not have to overcome perimeter defenses designed for external attackers.

Attackers can also be viewed as amateurs or professionals. Many people probably visualize an attacker as the stereotypical male teenage "hacker" perpetuated by the mass media. While amateur hackers are undoubtedly responsible for a substantial fraction of viruses and worms and other vandalism, the involvement of professionals and perhaps organized crime is suggested by the sophistication of attacks and number of attacks apparently driven by profit motives (Swartz, 2004). Besides professional hackers, other professionals involved in electronic attacks include national governments, military agencies, and industrial spies.