Chapter VII

Security Threats and Vulnerabilities

Introduction

Perhaps some of the biggest security problems facing all of us using computers and other information systems are the security threats and vulnerabilities that an average computer user has little to no idea about. Even those who have some knowledge of these threats are still in the dark as to how prepare for and avoid them. The focus of this chapter is to explain what these are and how to deal with them in our everyday activities.

A security threat to a computing system is a set of events that do not actually exist yet, but are likely to happen, with the potential to cause harm or loss. For example, heavy sustained rain in areas prone to flooding creates a threat of flooding. A vulnerability, on the other hand, is a flaw or weakness currently existing in the system, the security procedures, design, or implementation that
could be exploited intentionally or accidentally, resulting in a loss or harm. For example, a broken lock on a door is a vulnerability, because, if known by a thief, it can be exploited to enter the house and cause a loss to property. Finally, a control is a mechanism used to prevent a threat by controlling the vulnerabilities. For example, buying a new lock and replacing the broken lock on the door with it is a control.

**Types of Threats and Vulnerabilities**

Considering the nature of information systems, there are many threats and vulnerabilities that we cannot humanly list; however, we can consider the types in groups their nature groups starting with the vulnerabilities.

**Types of Security Threats**

There are numerous security threats originating from many different sources and based on a variety of motives. All these threats can be grouped into a few types that include disruption, destruction, disaster, unauthorized access, interruption, interception, fabrication, and modification. Others are threats resulting in loss of use, loss of performance, disclosure of information, and loss of integrity:

- **Threats resulting in loss of use**: Can be due to an interruption of service, as in denial of service, theft, vandalism, fire, and natural catastrophes.
- **Threats resulting in loss of performance**: May result from interruption, modification, and fabrication. Interruption may be caused by a denial of service, which may degrade the performance of the system. Modification of system code and data, as a result of unauthorized access, may lead to performance degradation in the system.
- **Threats resulting in disclosure of information**: Many times disclosure of information is a form of interception, resulting from unauthorized access to the system, which may lead to illicit copying of critical information. It also may result from accidents and sometimes human error. Recently, disclosure of information is becoming a big problem,
Performance Evaluation of Web Server's Request Queue against AL-DDoS Attacks in NS-2


www.igi-global.com/article/performance-evaluation-of-web-servers-request-queue-against-al-ddos-attacks-in-ns-2/187075?camid=4v1a