IDEA GROUP PUBLISHING **ITB11410**

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 chapter appears in the book, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* by Lech J. Janczewski and Andrew Colarik © 2005, Idea Group Inc.

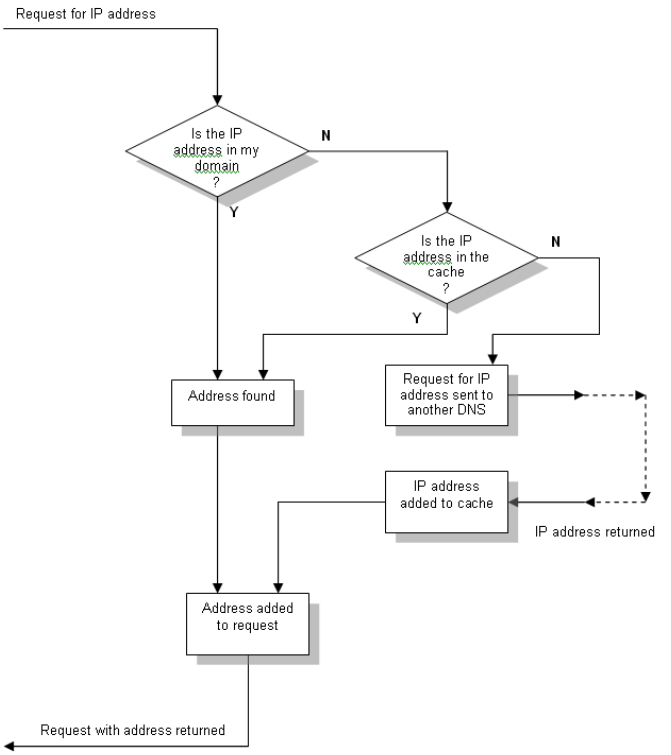
Chapter 7

DNS Attacks

The Domain Name Service (DNS) is a mechanism for recognizing and translating domain name addresses. These operations are carried out by devices called Domain Name Servers. Thus, DNS attacks are attacks against the Domain Name Servers.

As human beings, we prefer to operate with addresses such as *www.auckland.ac.nz* rather than *130.216.96.3*. The numeric representation is harder for us to remember than a meaningful representation. However, the underlying protocols of the Internet prefer 1s and 0s. To help us, a DNS is used to map the domain name to the numeric equivalent address (i.e., www, ftp, e-mail, etc.) where a given server awaits our request. When a request is made to a given domain, the request is translated by the DNS, and the equivalent IP address of the host server is returned. Internet DNS servers are arranged in a distributed manner so that if one server does not have the mapping, it may request the mapping from other DNS servers. If the mapping is requested from another server, then the requesting server stores a cached copy of the mapping for a limited period of time to be used for providing subsequent queries. Figure 7.1 shows the logic of the DNS operation.

Figure 7.1: Logic of DNS operations



Launching an Attack

How can a DNS attack be launched? The DNS protocol has virtually no authentication method that provides a means to ensure the identity of both sides of a given transaction (i.e., the requesting client and the DNS server). In the headers of the DNS query and response, there is a 16-bit field that is used for the identification of a query. However, there is no way of determining if the returned message contains a real IP address or if the entire message was sent by a real DNS server. So the whole game is about convincing the DNS client that the received message is genuine. The query IP is generated (in this 16-bit field) sequentially, and predicting future values is trivial through monitoring the communications. When the next query is sent, an attacker can send an