What If?

eGlobal Bank is a reputable bank in New York City with a large number of co individuals as customers. In addition to regular banking services, the bank bega number of online services that included online bill payment, transaction of mo credit cards, and other online transactions.

Recently, Web hacking attacks on institutions in the financial sector have increa These include attacks that access the personal information, credit card details, and bank account details of bank customers.

Due to the growth of such incidents, eGlobal Bank made the security of its bankin a top priority. The bank had basic experience in security, so it had a firewall install party. The bank believed that its banking sector was completely safe from the vuln Web attacks.

A few months later, bank officials were taken aback by the news that their serve hacked and sensitive information on thousands of customers had been stolen.

- How did the attacker access the servers despite the installation of a firewa
- How might an IPS have prevented this breach?

Introduction to Evading IDS, Firewalls, and Detecti Honeypots

This chapter focuses on evading IDS, firewalls, and honeypots, security features t trators deploy to protect their networks. It covers each of these features and the se involved with each.

Introduction to Intrusion Detection Systems

Attackers are always on the prowl to compromise networks. This poses a majo company's internal network.

One of the simplest ways of preventing attackers from compromising a network i ize its settings. Customization of network settings gives network administrators means of monitoring network traffic. Administrators can also put restrictions and information exchanges taking place over the network to prevent unknown an ticated users from accessing it.

It is also necessary to understand the importance of continuous monitoring. Havi or intrusion detection system on a network does not make the network secure u continuous monitoring of the exchange of data information and network traffic. network administrators must be thoroughly trained to track log files, look for su natures, and maintain a database of weekly alerts. This allows them to track ever occurred over a specific span of time. This information gives systems personnel t