Arp poisoning case study example

Business, Company

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Introduction

With the electronic world that we have today, email communication remains one of the most essential tools that are used for communication. It forms the backbone of communication in many organizations. The use of email will grow from time to time. As the growth is seen to be exponential, its security is an important aspect that should be considered. The security implications of email storage, the policy implementation and enforcement and data recovery are the issues that are being considered today. In order to avoid failures, there is need to manage large data information in a well-organized and secure manner .

Man-in-the-middle attacks

This is an attack which is common in local area networks. This attack is a form of active and aggressive eavesdropping where the attacker will create independent connections between the parties communicating so that the attacker will feign either parties communicating. In the end, the parties communicating will think that they are having a private communication and yet in the real sense, the communication is being controlled by the attacker.

MAC flooding

MAC flooding is ARP cache poisoning technique that is targeted at switches. There is a difference between switches and hubs. Switches send network packets to particular host that was meant to get the information. Hubs just rebroadcast all the information and traffic they get. They do not have a mechanism which will enable them to check where the traffic is headed. There are some switches which go to hub mode when they become overloaded. Hackers will take advantage of this by ensuring that traffic is overloaded to the switch so that they get access to the traffic and therefore be able to packet sniff the network. This is possible when the switch is in the hub mode.

References

Tan, C., & Ruighaver, A. (2005). A framework for investigating the development of security strategy context in organizations. Conference Proceedings of the 6th Australian Information Warfare and Security Conference: Protecting the Australian Homeland (pp. 216-226). Sydney: Deakin University.

Tan, C., & Ruighaver, A. (2004). Developing a framework for understanding security governance . Second Australian Information Security Management Conference Proceedings (pp. 1-11). Sydney: Edith Cowan University.