Network Security

Contributed by Administrator
Friday, 18 August 2006
Last Updated Tuesday, 23 January 2007

External attacks by hackers, viruses, worms and trojans are permanent threats to any progressive company. What is not widely known, though, is that the major portion of attacks come from within the network.

In 2002 KPMG reported that up to 80 % of all intrusions were initiated internally, from inside a company network. Technical ignorance, curiosity and intentional manipulation of data often lead to serious damages for organisations.

Internal network attacks are typically operated via so called ARP Spoofing or ARP Poisoning attacks. Malicious software to run ARP Spoofing attacks can be downloaded on the Internet by everyone. Using fake ARP messages an attacker can divert all communication between two machines with the result that all traffic is exchanged via his PC. By means of such a man-in-the-middle attack the attacker can in particular

· Run Denial of Service (DoS) attacks
· Intercept data
· Collect passwords
· Manipulate data
· Tap VoIP phone calls

These ARP attacks are usually successful even with encrypted connections like SSL, SSH or PPTP. ARP belongs to the OSI data link layer (layer 2).

Here is a a non-technical description of ARP attacks:
When computers exchange data with each other, the so-called IP-address comes to play. It is a logical address, to which data packets are sent. Next to this, each computer - or more correctly its network card - has an unique physical address, the MAC-address. The ARP-tables define the connection between these two addresses (ARP = address resolution protocol). Each logical IP-address has its physical MAC-address counterpart. If any of these table entries are exchanged, so-called man-in-the-middle attacks become possible. This means that data streams are routed unnoticed via the attacker's computer. Here the data can be read or manipulated.

In the meantime there are even attacking tools available on the Internet. Every skilled network administrator can execute professional ARP attacks. Without any precautionary measures by the organisation that is running the network, the risk for the attacker to become unveiled is close to zero. Encryption, like used e.g. with online banking, is not offering any protection against ARP attacks. ARP spoofing attacks are operated either from within the network, for instance by employees or contractors, or a small device can be installed within the network and the attacker controls this device remotely. Placing the network device does not require any specific skills, cleaning personnel or housebreakers are sufficient.

ARP spoofing is a particularly refined method to attack computer networks of all kind. It should be noted that attacks of this kind are almost impossible to detect.