

[fw-wiz] Defense in Depth to the Desktop

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-12/0023.html>

From: Chris Pugrud (cpugrud_at_yahoo.com)

Date: 12/02/04

To: firewall-wizards@honor.icsalabs.com
Date: Thu, 2 Dec 2004 11:24:28 -0800 (PST)

Defense in Depth to the Desktop
the Strong Internal Network Defense model

Most organizations have expended large amounts of money and resources in strengthening their perimeter defenses, primarily through firewalls and similar network hardware mechanisms. Additionally, most organizations rely only on operating system security controls for the internal networks, not applying strong internal security controls. The lack of strong internal security controls is highlighted when the internal network and systems suffer catastrophic failure when attackers, malware, and, most destructively, worm viruses make their way into the network inside the defensive perimeter. This is the classic "eggshell" weakness of network security, hard and crunchy on the outside, soft and chewy on the inside. The Strong Internal Network Defense (SIND) model attempts to address this key vulnerability through the application of hard internal defenses through network hardware.

Overview

Consider the following example of a simplified network. The network is divided into two subnets; one subnet contains all of the client systems, while the second subnet contains all of the servers. The client subnet and the server subnet are separated by a session based, stateful, packet filtering firewall. The firewall is unidirectional; it only permits traffic that is initiated from a client to a server. Servers are allowed to reply to clients, but they can not initiate communication, TCP or UDP, to a client.

Surprisingly, this example does not break Microsoft or most application [*1] protocols. The result is counterintuitive, but analysis and testing support this assertion.

In addition to the firewall, the client systems are fully isolated from each other by layer 2 controls (private vlans). The servers may be similarly isolated, but doing so is minimally effective and damaging to server to server communications.

Consider the introduction of a zero day worm virus [*2] into such a network by

Firewall–Wizards: [fw–wiz] Defense in Depth to the Desktop

an infected client. The client can attack all of the servers, and all of the servers may become infected. The infected client can not attack any of the other clients because of the layer 2 isolation. The infected servers can not attack any of the clients because of the firewall. The end result is that one client and the servers, a small subset of the organization, are infected. This is much less devastating, and much easier to clean up, than if the entire network was infected.

[*1] MAPI, the protocol used by MS Exchange clients (outlook)