CPA
Practice Advisor

before and she knew it well. The system was easy to access even with the low-end firewall installed on the router.

Apr. 17, 2008

From the April/May 2008 Issue

Deep-Penetration, a hacker’s nom de plume, had been to this network address before and she knew it well. The system was easy to access even with the low-end firewall installed on the router. Even if the firewall had blocked her ability to access the network, the person configuring the router/firewall hadn’t changed the default administrative password. She could have easily used this to access the network by simply looking in the User Manual on the manufacturer’s website.

The administrative password on the server was still the default password known to everyone, and no one installed Service Pack 2, which would have disabled the administrative account. It was easy pickings. Deep-Penetration had even figured out how to access the tax application that was installed directly on the machine she was using to connect to the internal network. She enjoyed looking at all the personal financial details.

On previous visits, she had found several high net worth clients who had more than one million dollars in income. This time, Deep-Penetration was back for a reason. She had seen a posting in a hacker forum saying that a hacker going by the name of ID-ME was paying $600 per name and matching social security number.

Deep-Penetration was short on cash and figured selling some names and social security numbers to ID-ME would be a quick way to make some money without getting caught. She knew exactly where she could get at least 2,000 names and the matching

understand this very important security prevention technique — what I like to equate to putting a dead bolt on the door. And they may not know if their firms are as prepared as the owners might assume. The scenario above identifies a lot of things that are wrong besides the firewall. However, these mistakes could very well be happening in a firm and no one knows it. With what seems like every vendor coming out with a firewall as part of their product offering, many people may think that they are over protected. Unfortunately, this idea lulls us into a false sense of security.

The Types of Firewalls

Good news! Firewalls only come in two basic designs: software-based and hardware-based.

While each has its strengths and weaknesses, some basic things are designed into certain firewalls that make them more secure than others. We will talk about that aspect shortly, but first let's make sure we are on the same page in terms of definitions.

A **hardware-based firewall** is a physical device that connects to your Internet router and sits between your local area network (the computers and servers that make up your technology environment) and the Internet. It allows traffic in and out between the local area network and the Internet based on the rules defined on the device. A hardware firewall generally stops traffic at the perimeter between the Internet and the internal network. It does not monitor the traffic on the internal network.

A **software-based firewall** is a firewall installed on a computer or server. It monitors the physical network connection of the computer as it connects to either the local area network or the Internet. It is also rules-based just like a hardware firewall. Generally, software-based firewalls are much more open because they have to communicate not only with the Internet but also

With all the software firewalls, it is a miracle that we are able to connect to the network and Internet at all. And this is the exact reason that software firewalls generally do not function well for us. They are, by default, fully or mostly open in order to pass traffic back and forth without much configuration by the user. They do little to protect us.

Unless a user spends time configuring the firewall properly and making the default settings more restrictive, it is pretty much open season on a computer running a software firewall. In short, unless you take specific action to check and configure the firewall settings on your software firewall, do not assume that it is providing much protection.

Hardware Firewalls
This category of firewall is a device designed to be used as an intermediary between a local area network and the Internet. This type of firewall controls the traffic passing through it, preventing unauthorized traffic from entering the system and allowing authorized traffic through to the computers attached to the network.

Hardware firewalls generally have an Ethernet connection to the Internet and a second (or perhaps multiple) Ethernet connection(s) to the computers in the firm’s local area network. Because the hardware firewall is a specific device with two Ethernet ports that connect together to different network segments (Internet and local network), it monitors the activity between the two network types while the software firewall only monitors a network connection on a specific device.

Which is Better?
Because hardware firewalls provide a physical separation between the computer(s)

on the local area network and the Internet, a hardware firewall is much better

except that which is specifically allowed.

Software firewalls also have a secondary vulnerability. Should there be a security vulnerability on the computer where the software firewall is installed either within a piece of software or the operating system, the firewall can be bypassed using this vulnerability. The hacker now has access to the machine even though the software firewall is "monitoring" the connection.

Hardware firewalls are configured using the same two methods listed above; however, the high-end hardware firewalls follow option 1 configurations and specifically block everything unless it is allowed by the user. The hardware firewall's physical separation of network segments makes it harder to bypass the firewall device and access the computers on the internal network segment. Hardware firewalls, since they are separate pieces of equipment, are not susceptible to software vulnerabilities on a computer. Network traffic must pass through the hardware firewall before it reaches a computer with a software vulnerability. This provides a much higher level of protection to the internal network.

What's Next?
In our next issue (June/July), I will finish the story about Deep-Penetration and what happened with the information she obtained from the unknowing firm. And along the way to finishing the story, we will examine which firewalls should be used in accounting firms and which firewalls should be avoided.

Technology