Knowing the ways of the enemy

METHOD OF ENTRY

Most users have become so accustomed to networking that they never stop to ask if anyone may be listening. We all know we'd better be careful on the open Internet – even home users now use firewalls to keep intruders off the wires, and corporate admins throw in a Maginot line of proxy servers, honeypots, and tools of the DMZ.

But what's happening *inside* the firewall? How will you know if someone is listening – or maybe even impersonating another user? Statistics tell us that many attacks begin on the inside, from bored or disgruntled employees looking for a thrill, or possibly, from an even angrier sort looking for some form of revenge. In many corporate settings, a complete stranger can show up with a laptop and plug it to the network without exciting any response at all from the security system. The problem is even worse with wireless networks. A casual vandal standing across the street, or even in the next apartment, can make contact with your network.

But how do these intruders convert access to entry? How do they trick your systems into letting them use the network medium for their attacks? We'll provide you with answers to that question in this month's Security cover story.

Our leadoff article looks at techniques intruders use for attaching wireless clients. We'll show you how an attacker can hijack a wireless connection. You'll also learn how an enterprising intruder can pretend to be a secure network and get an unsuspecting client to connect. And we'll show you the remarkable Hotspotter tool, which will demonstrate just how vulnerable your wireless network really is.

Our second article examines the dark art of ARP spoofing. ARP spoofing lets an intruder use a fake MAC source address to impersonate another computer on the network. You'll also learn about MAC flooding attacks, which target the security mappings of a network switch, and ARP poisoning, a special form of spoofing that attacks the ARP table of another computer. We'll show you why even SSL and SSH are not immune from ARP attacks, and we'll describe some ARP exploit tools used by real intruders on real networks. We'll finish with tips on how you can protect your network from the dangers of ARP spoofing.

To round out this month's Security cover story, we take a look at the Simple Security Policy Editor (SSPE), a handy tool that helps you organize and maintain security policies across multiple firewalls. The free SSPE offers a very simple front end that lets you configure and administer a complex distributed firewall environment.

We hope this month's Security cover story brings you new insights and new ideas for how to make your own network more secure. ■