Hack Proofing Your Web Server

by Erik Petersen

Most people think firewalls are all they need to secure their IT investment. Firewalls are very important, but they are just one piece of the overall security picture. Even with perfect installation, configuration, and maintenance, firewalls still must allow access to your public web servers. Hackers know how to use this permitted access to gain the foothold they need to gain access to your network. The kind of access a web server can give them is nothing short of complete administrative control. So when your organization decides to host a web server, you should understand that the server is fully exposed to attack, even if it is behind a top notch firewall. The most critical step towards protecting your public servers from attack is to harden the servers and turn them into bastion hosts.

So what is a bastion host? A bastion host is a server that is configured very differently from typical servers. Typical servers run hundreds of services and programs that are not needed. Most of those services and programs are vulnerable to attack. The premise for building a bastion host is that the server can be divided so that each of its partitions fulfills a specific role. Once that role is understood—web server, mail server, middleware server, etc.—the partition can be secured to serve only that role. All the unnecessary services, executables, protocols, programs, and network ports can then be disabled or removed.

------ **If your web server is running on a default installation, you either are going to be hacked, or you are currently hacked**----

Building a bastion host is not easy. If the server you are trying to harden is running on Windows NT, or Windows 2000, you have an especially tough road ahead. Win2k and NT are very difficult to harden, but they, especially, must be hardened since more than with Linux or UNIX, the default installation turns everything on. Your job is to turn almost all of it off. Do you really want web server based printing running? Or web based password administration? Of course not, yet the default installation for Windows NT and Windows 2000 turns these functions on, as well as a couple hundred other dangerous configurations as well. This is why the Internet world lost almost a billion dollars to Code Red and Nimda last year. If your Microsoft server was properly hardened, you would not have been affected by either Code Red or Nimda, even if you had neglected to install Microsoft's security patches. Microsoft security patches are great, and all administrators should religiously keep up with them, but only server hardening will protect you from future outbreaks. What to turn off and what to remove is the trick.

At Polar Cove we have our own system for hardening servers, and our own standard. Our standard exceeds those of the National Security Agency and the F.B.I. The NSA standards are excellent, and very high, but we have found that more could be done, and so we protect or harden an additional 63 settings. It is important to have a standard in mind; otherwise you will have difficulty measuring your results. As it is with any security plan, it is important to prove, via some sort of measurement and standard, that you did, in fact, accomplish the security you intended.

Why Harden Public servers?

(1) It reduces the likelihood of successful intrusions or attacks.
If you harden to NSA, or other strict standards, you protect yourself from prosecution or regulatory sanction by demonstrating compliance with an accepted prudent due care security standard.
(2) It verifies secure configuration of your systems prior to network deployment, and prior to

exposure to attack.
(3) You can demonstrate to management that your system security measures up against high security benchmarks and standards.
(4) You will be able to require your business partners to comply with a high security standard.

Using these three steps, securing, alerting and auditing, together can increase the level of security of your company's most valuable asset: its data.