THE PROC DIRECTORY - SECURITY MODIFICATIONS

Linux has a wonderful facility in the /proc directory. This directory allows the system administrator a real-time access window into the workings of the kernel. The files here are therefore referred to as a "Virtual File System", as the files are representations of different kernel configurations. You can view view some, to see exactly what is happening on your server. Or -as we will discuss- you can modify them, and thus modify the running kernel in real-time. We will be looking at some of the switches relating specifically to securing your system. Please bear in mind that these are general recommendations, and not all these settings may be benefical to you, so please test any changes throughly, and at your own risk.

- */proc/sys/net/ipv4/conf/*/rp_filter*
  Setting this switch to 1 will enable reverse path filtering to help stop any IP spoofing attempts.

- */proc/sys/net/ipv4/conf/*/log_martians*
  A "martian" is a packet which arrives at an interface, but the server has no route to the specified source address. Packets like this should not exist, so set this option to 1 and log them.

- */proc/sys/net/ipv4/tcp_syncookies*
  Setting this switch to 1 will enable protection against SYN floods.

- */proc/sys/net/ipv4/icmp_echo_ignore_broadcasts*
  There is no reason to allow icmp broadcasts. The most common usage for them is to run DOS attacks. Set this switch to 1 to get your server to ignore them.

- */proc/sys/net/ipv4/conf/*/accept_source_route*
  Source routing is bad, only attacker would want to explicitly state how there packet is routed. Disable this by setting this switch to 0.

- */proc/sys/net/ipv4/conf/*/accept_redirects*
  There are very, very few legitimate situations where your host should actually be getting route redirects messages. Disable this by setting this switch to 0.

- */proc/sys/net/ipv4/icmp_ignore_bogus_error_responses*
  Sometimes some devices will send invalid responses to what they percieve as broadcasts. These responses are non-RFC compliant. Ignore these by setting this switch to 1.

- */proc/sys/net/ipv4/icmp_echo_ignore_all*
  If you have no need for your server to respond to any icmp traffic, then enable this by setting this switch to 1.

- */proc/sys/net/ipv4/tcp_timestamps*
  TCP timestamps can provide a source of information for attackers. On secure servers disable this by setting this switch to 0.

- */proc/sys/net/ipv4/conf/eth1/send_redirects*
  This switch should only be enabled if you're a router advertising alternate routes to your network. In all other cases disable this by setting this switch to 0.

- */proc/sys/net/ipv4/conf/*/secure_redirects*
  This switch should only be enabled if your server exists in a large, multi-router, dynamic routing network. For all cases disable this by setting this switch to 0.

- */proc/sys/net/ipv4/ip_forward*
  This switch should only be enabled if you're got a server which needs to route packets between it's network interface cards. In all other cases disable this by setting this switch to 0.

- */proc/sys/net/ipv4/conf/*/proxy_arp*
  This switch should only be enabled if you're got a server which needs to respond to arp packets. This switch will enable the server to respond to any arp packets destined for addresses which the kernel has routes to, useful for bridges. In all other cases disable this by setting this switch to 0.