

# SecurityFocus Article Announcement

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2003-03/0085.html>

---

**From:** Hal Flynn ([flynn@securityfocus.com](mailto:flynn@securityfocus.com))

**Date:** 03/27/03

Date: Thu, 27 Mar 2003 09:06:11 -0700 (MST)

From: Hal Flynn <[flynn@securityfocus.com](mailto:flynn@securityfocus.com)>

To: [focus-linux@securityfocus.com](mailto:focus-linux@securityfocus.com)

Incident Response Tools For Unix, Part One: System Tools

By Holt Sorensen

This article is the first in a three-part series on tools that are useful during incident response and investigation after a compromise has occurred on a OpenBSD, Linux, or Solaris system. This installment will focus on system tools, the second part will discuss file-system tools, and the concluding article will look at network tools.

<http://www.securityfocus.com/infocus/1679>

Cheers,

Hal Flynn  
Symantec Corp.

"...You guys are the Marine's doctors; There's no better in the business than a Navy Corpsman...."

— Lieutenant General Lewis B. "Chesty" Puller, U.S.M.C.