

## re: ridiculous situation

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-11/0750.html>

---

**From:** H C ([keydet89@yahoo.com](mailto:keydet89@yahoo.com))

**Date:** 11/29/02

Date: Fri, 29 Nov 2002 06:31:16 -0800 (PST)

From: H C <[keydet89@yahoo.com](mailto:keydet89@yahoo.com)>

To: [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)

Harley,

Perhaps I'm not seeing where your problem lies. From what you describe, you have 5 systems that you've recently inherited, and they've been largely unprotected since they were first turned on.

"you can't simply firewall them off and leave them for dead."

What are you saying? Are they business critical? If so, determine what services each of them should be providing, and then disable/restrict/limit the available running services to just those. Think about adding tcpwrappers, as well.

Examine the configurations of the machines, and see what's going on. What is the level of the kernel? Would it be worth the time to upgrade? If the systems are business-critical, you'll likely have to schedule maintenance for after hours. Is the default kernel image in place, or were the kernels recompiled specifically for each machine?

"how would you be sure there are no trojans, bots etc...chkrootkit and so on, i suppose, but how reliable will the results be?"

What do you mean? You could always do the checks by hand yourself...it would take more time, but perhaps be more reliable.

If I were you, I'd start w/ a security assessment of each machine. Check for setUID files, running services/processes, examine the configuration. Examine the syslogs, see what's currently there. Once

## SecurityFocus BASICS: re: ridiculous situation

you've completed your examination, develop a plan to tighten things up...it may take a while, b/c you'll have to determine the business processes that use these systems. You want to make sure that you don't disrupt those processes in your efforts to secure these systems.

Your situation isn't so much ridiculous as it is pretty normal...

---

Do you Yahoo!?

Yahoo! Mail Plus – Powerful. Affordable. Sign up now.

<http://mailplus.yahoo.com>