Network at MIT - Security Primer for UNIX System Administrators

Network at MIT - Security Primer for UNIX System Administrators

Context

Achieving reasonable security for multi-user systems (such as UNIX) takes time and effort, and once implemented, requires periodic review. It's not remarkably difficult, but does require a certain throughness of effort. Security is often an endeavor where a 90% effort is the same as no effort at all.

In case of a break-in

Outlined here are steps to take when you discover a break-in on a machine you administer.

What to do if you realize your password or system has been compromised.

Frequently Asked Questions

Q: How should we make our network secure?

Owners, administrators, and users of machines on MITnet must make reasonable efforts to protect their computers. This includes:

- Correctly configuring the operating system to eliminate security holes.
- Choosing and using good passwords, that are not easy to guess or crack.
- Keeping abreast of (and correcting!) newly identified weaknesses in the operating system, and other threats:
    - The Computer Emergency Response Team (CERT) at Carnegie Mellon University issues advisories detailing system weaknesses and how to correct them, along with other security information. Worth checking for information about your operating system.
    - Subscribe to the **netusers** mailing list, a low-traffic list where significant network events, like outages or security notifications, are sent by the operations staff. You can subscribe by the Athena mailmaint program, or by sending mail to netusers-request@mit.edu.
- Never sending passwords or other sensitive information over the network in the clear.

See More

- The Bugtraq mailing list is for detailed discussion of UNIX security holes: what they are, how to exploit, and what to do to fix them. You may subscribe to the list by sending email to listserv@netspace.org with the words **subscribe bugtraq** in the body of your message.
- The Best of Security mailing list is a compilation of the interesting information from several other security-oriented mailing lists. You may subscribe to the list by sending email to majordomo@suburbia.net with the words **subscribe best-of-security** in the body of your message.
- linux-security@redhat.com discusses security holes in Linux. To subscribe, send mail with **subscribe** as the subject to linux-security-request@redhat.com. This list is archived in the net-defense discuss meeting on bloom-picayune.mit.edu.