A new Request for Comments is now available in online RFC libraries.

BCP 55
RFC 3227

Title: Guidelines for Evidence Collection and Archiving
Author(s): D. Brezinski, T. Killalea
Status: Best Current Practice
Date: February 2002
Mailbox: dbrezinski@In-Q-Tel.org, tomk@neart.org
Pages: 10
Characters: 18468
Updates/Obsoletes/SeeAlso: None

I-D Tag: draft-ietf-grip-prot-evidence-05.txt

URL: ftp://ftp.rfc-editor.org/in-notes/rfc3227.txt

A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

This announcement is sent to the IETF list and the RFC-DIST list. Requests to be added to or deleted from the IETF distribution list should be sent to IETF-REQUEST@IETF.ORG. Requests to be added to or deleted from the RFC-DIST distribution list should be sent to RFC-DIST-REQUEST@RFC-EDITOR.ORG.

Details on obtaining RFCs via FTP or EMAIL may be obtained by sending an EMAIL message to rfc-info@RFC-EDITOR.ORG with the message body help: ways_to_get_rfcs. For example:

To: rfc-info@RFC-EDITOR.ORG
Subject: getting rfcs

help: ways_to_get_rfcs

Requests for special distribution should be addressed to either the author of the RFC in question, or to RFC-Manager@RFC-EDITOR.ORG. Unless

specifically noted otherwise on the RFC itself, all RFCs are for unlimited distribution.echo
Submissions for Requests for Comments should be sent to RFC-EDITOR@RFC-EDITOR.ORG.  Please consult RFC 2223, Instructions to RFC Authors, for further information.