CERT Incident Note IN-98-05: Probes with Spoofed IP Addresses

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Probes with Spoofed IP Addresses

Wednesday, November 24, 1998

The CERT Coordination Center has received several reports that intruders are using spoofed IP addresses to conduct scans similar to those discussed in

> http://www.cert.org/advisories/CA-98.09.imapd.html
> http://www.cert.org/advisories/CA-97.09.imap_pop.html

At first, these probes appeared to be ordinary IMAP scans. After further investigation, most of these sites determined that another compromised host on the same network was the true origin of the IMAP scan. It's possible that the intruder was able to run a network sniffer to capture the results of these probes.

If IMAP (or other) probes are reported to originate from hosts at your site, it may not be sufficient to disconnect the apparent origin from the network. We encourage you to inspect other hosts on the same local area network, especially if you continue to receive reports of intruder activity involving your systems.

You may find our Intruder Detection Checklist to be a useful guide in checking your systems for signs of compromise. This document is available from our ftp server at

> http://www.cert.org/tech_tips/intruder_detection_checklist.html

This document will help you to methodically check your systems for signs of compromise and offers pointers to other resources and suggestions on how to proceed in the event of a compromise.

Another approach to determine the true origin of spoofed probes is to install network monitoring software which can capture the packets actually traversing the network. Some network monitoring software logs may include the hardware (ethernet) address of the true origin of the probes. This information may enable you to determine which system is generating the spoofed probes by comparing the hardware address with those of other systems on the local area network.

While probes fitting this profile have thus far originated only from port 65535, it's possible that spoofed probes could come from other ports.

If you believe that your systems have been compromised and used to launch probes fitting this description, we encourage you to report the activity to the CERT/CC. In particular, we are interested in receiving copies of any intruder tools that have been used to generate spoofed probes or to capture the results.