The Apollo Incident: Summary.

Thomas Roessler <roessler@does-not-exist.org>

ABSTRACT

apollo.honeyp.edu was successfully attacked by an outside intruder who apparently planned to use the system as a base of operations for further attacks, and for activities on the Internet Relay Chat Network. The attacker tried to harvest user passwords, but was not successfull at this. There is no indication that apollo was actually used to attack remote systems.

1. Abridged Time Line.

apollo.honeyp.edu was attacked on Nov 7 2000, 23:11:51 CST. The intruder exploited a publicly known security hole and installed a simple back door on the system, which was later removed.

The intruder returned at 07:28 CST on Nov 8. He performed different kinds of activities:

- The intruder re-installed various system software packages in an attempt to harden the system against further attacks.
- The intruder replaced various system utilities with versions which would help to conceal his activities.
- The intruder compiled and installed a version of the Secure Shell server which would permit him to log in using a special password. As a side-effect, this version of the Secure Shell server would log any passwords entered.
- The intruder installed and ran an IRC client, and tried to install a "robotic" IRC client. Apparently, the attacker planned to use apollo for various IRC-related activities.
- The intruder left behind various tools which could be used to attack other systems, using apollo as his new base of operations.
- A network sniffer was run.

The intruder left the system at 08:06 CST.

The system's state was frozen at approximately 20:00 CST.

2. Impact.

No user passwords were collected by the intruder. There are no indications that the host was actually used to attack other systems.

An in-depth investigation of the incident took 37 hours.

3. Notes.

The break-in could have been avoided by applying vendor-supplied software patches in a timely manner. The weakness used had been publicly known since July 2000. The attack tool used was published on August 5. A vendor-supplied upgrade was available since July 17, 2000. In order to avoid future break-ins, steps should be taken to ensure proper software updates and systems administration.