23rd National
Information Systems Security Conference
16-19 October 2000
Baltimore, MD

Title or Topic: Information Security Year in Review--Technical Vulnerabilities

Abstract

A 90-minute review of the major technical vulnerabilities discovered in systems during the previous 12 months (Oct 99-Sep 00). The tutorial will include discuss categories of technical problems and draw from CERT advisories, hardware and software vendor's advisories and public discussion forums. The intended audience is Information Security (IS) managers and practitioners who are too busy monitor all of these forums. The tutorial will provide a snapshot of major problems and trends that have emerged since the last NISSC. The tutorial may follow this outline adapted from the 21st and 22nd NISSC tutorials:

- Good News
- Bad News
- System Scanning
- 2000, Year of the Buffer Overflow (Nth Iteration)
- Denial of Service Attacks Continue
  - Distributed Denial of Service Attacks
  - Cryptography-related Denial of Service Attacks
  - Should We Worry about Denial of Service Attacks?
  - Who Should Worry about Denial of Service Attacks
- UNIX vulnerabilities
- NT vulnerabilities
- Trojans and Backdoors
- Solutions
- Forecast for 2001

While 2000 looks remarkably similar to prior years with respect to the broad categories of problems that continue to plague IS professionals, denial of service attacks seem to be on resurgent. The tutorial itself reviews specific new problems that may be instances of the old classes of vulnerabilities. If a new major category of technical problem surfaces, the tutorial will include it. Heap overflows be an example.

Author(s): David Kennedy CISSP

Organizational Affiliation: Director of Research, ICSA, Inc.

Phone numbers (voice and fax): v: 513.779.7412 f:513.779.7413

E-mail address: dkennedy@icsa.net