Security Incidents Report

Reporting Period: April - June 2002

Prepared for: Eugene Siciunas
Director
Computing & Networking Services
University of Toronto

Date Prepared: October 17, 2002

Computer Security Administration
Computing & Networking Services
University of Toronto

Contents

Background Information

One of the goals of the Network Security Policy is "to provide an effective mechanism for responding to external complaints and queries about real or perceived abuses of University networks and computer systems." The Director of CNS tasked the Computer Security Administration to establish a Networks Contact database and to seek input from System Administrators across campus to provide the necessary contact information to populate the database and to maintain the database up-to-date through periodic revisions of the contact information.

Computer Security Administration designed and implemented an Access database and populated the database with information supplied by System Administrators. System Administrators can request changes to the database data by sending e-mail to security.admin@utoronto.ca or by submitting the "Network Contact Database Update" web form available at the CSAG web page at http://www.utoronto.ca/security/network_contact.html.

In May of 2001, Computer Security Administration starting using the Remedy reporting facility available through the Network Management Support Systems group of CNS. With assistance from the group, an Incident Tracking form was designed, tested and implemented. This form enables CSAG and other CNS staff to document and review Security Incidents.

The Security Incident Tracking form includes information such as report date, information about the individual submitting the incident report, affected network(s), information on the network from which the incident originated, action(s) taken to resolve the incident and other pertinent information.

This reporting facility enables CSAG to track incidents and maintain a history of security incidents. This information will enable CSAG to provide periodic statistical analysis reports to management and to keep management informed on the magnitude of problems associated with such incidents.

Ultimately, this process will enable the University to respond more effectively to security incidents and thus minimize or at least contain any damage that such incidents could bring to the reputation of the University.

Overview

This report covers the period from **April to June 2002**.

It is important to keep in mind the following disclaimers:

- The report only reflects incidents that were reported to Computer Security Administration.

   Although the Information Commons Postmaster and abuse reports collection points within CNS are forwarding incident reports to Computer Security Administration, not all incidents are being reported to Computer Security Administration and therefore are not reflected in this report.

The procedure being used to record and respond to reported security incidents follows:

- When a report is received, it is recorded in Remedy.
- The report is acknowledged. A canned message is sent to the person submitting the report. The message includes a unique UTCSA Security Incident Tracking number (automatically assigned by the Remedy system).
- The contact for the network from which the abuse originated is also notified. And a canned message is sent to him/her. The message includes the unique UTCSA Security Incident Tracking number.
- The administrators of any other affected networks are notified.
- The incident is tracked and actions taken to resolve the incident are recorded in Remedy.

During the three-month period covering April to June 2002, we created **303** incident reports.

In all, Computer Security Administration handled approximately **594** e-mail messages during this reporting period.

Network Scans

CNS now runs regular scans of networks and has implemented a secure web-based delivery system for scan reports. System Administrators are now able to log in to a secure site to view reports of scans conducted by CNS. This site is also being used to post information about malicious code and other information of interest to system administrators.

Scanning is an active process. Intrusion Detection is passive Monitoring. However, the two are interconnected. Scanning enables us to identify actual and potential exposures and this enables system administrators to

take pro-active measure in securing their systems. Statistics are used in intrusion analysis.

Network Security Sweeps

The Nessus scanner is used for the security sweeps. Full scans are done once every month. Incremental scans are done on an as-need basis, for example, when new exploits are released or when new vulnerabilities are found. We also do scans "by request" when system administrators submit a request following an incident or after they have made changes to their environment.

We are not currently tracking changes between scans.

Scan reports are presented in a cross-referenced html format and are made available for more than 134 network administrators.

Currently, Nessus performs over 850 checks. We are scanning mostly for "High Risk Vulnerabilities" and related information. For example, the scanner has checks for IIS specific vulnerabilities (exploited by CodeRed/Nimda).

Not all of the hosts appeared in every report. We send notification messages to network administrators when vulnerable IIS hosts are detected. This enables them to react quickly and thus reduce the number of incidents we have to handle.

We are also using information from the scan reports when the Intrusion Detection System detects something suspicious. This enables us to identify false positives. It also enables us to identify the way a system has been compromised.
For example, if the IDS detects a hostile activity such as a UNIX worm that may include buffer overflow attempts against various services (LPR, SSHd, statd, telnet, BIND, dtspcd, etc.) on the hosts, and if the host had been compromised, we know it was compromised because IDS registered a TCP port sweep from that host. If the scan report also found that the host was vulnerable to the "SSH CRC32 compensation attack", we could then conclude that it was penetrated via SSHd.

The information provided by the scans enables network administrators to find IP addresses of machines aggregated by a particular vulnerability or running service very quickly without doing a full scan themselves. They are also able to see the list of vulnerabilities for a particular IP. All these features and the way the scans are performed were developed by CNS as the Nessus scanner doesn't have report generation ability suited for an environment with multiple administrative contacts.

Intrusion Detection Systems Statistics

We are using open-source Snort IDS for this service.

26   notification messages were sent about Nimda
10   notification messages were sent about CodeRed
 1   non-21 FTP serv BINARY
 2   WEB-IIS cmd.exe access

39

Note: These incidents are also included in the statistics on Page 7.

Open Relay Scans

When the scans were first started, in July of 1999, there were seventy machines on campus that had open relays. Regular scans conducted since then have detected only the odd open relay.

Alerts Lists

CSAG has established two alerts lists in order to disseminate information about important security events to UNIX and Windows systems administrators. These broadcast lists have been used to distribute information on available patches for known vulnerabilities as well as information about new viruses and other malicious code.

Security Incidents Statistics (April - June)

Number of incidents recorded by type:

- DDoS[1]   26
- Hacking   13
- Harassing e-mail   3
- Malicious Code[2]   54
- Scan/Probe   24
- Spam   44
- Theft/Fraud[3]   3
- Unauthorized Access   1
- Unauthorized Use   4
- Other   131

Total   303

Number of internal incidents (originating from campus networks):   239

Number of external incidents[4] (originating from off-campus networks):   64

---

[1] Most of these incidents involved CodeRed & Nimda infected machines. In many cases system administrators hadn't installed available patches.

[2] SirCam and Klez virus incidents. The number of infected machines is higher than the number of incidents as some reports were for multiple machines.

[3] Unauthorized Distribution of Copyrighted Motion Pictures.

[4] These include incidents such as Spam as well as incidents involving forged IP numbers.