Security Incidents Report

Reporting Period: July - September 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 **July to September 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, other incidents are not 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 **July to September of 2002**, **342** separate incidents reports were created.

In all, Computer Security Administration handled approximately **574** 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 needed basis”, for example, when new exploits are released or when new vulnerabilities are found. Scans are also done “by request" when system administrators submit a request following an incident or after they have made changes to their environment. (Note: The frequency of network scans will be increased to every two weeks starting in October.)

Nessus security scanner is the primary scanning tool being used. Other tools are used to scan for particular vulnerabilities, for example, NBTEnum.exe and nbtdump.exe for blank windows passwords etc.

The total number of Nessus checks is now greater than 1090 (IP addresses/ranges are excluded from the scan by request.)

CNS participates in software problem investigation (when a server crashes during a scan for example) as problems may re-occur either as a result of the scan or due to probes coming from outside. When a problem occurs, the affected server is re-scanned and then the scan data is analyzed to determine the cause of the problem.

We notify system administrators about vulnerable machines during worm/exploit activity outbreaks for quick patching/disabling of affected servers.

Information provided by the scans is used to assess the current level of security and create necessary IDS rules/signatures.

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.

Not all of the hosts appear in every report. Notification messages are sent to network administrators when vulnerable IIS hosts are detected. This enables them to react quickly and thus reduce the number of incidents that have to be handled.

Information from the scan reports is also used 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. Also they are 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

An open-source Snort IDS is being used for this service.

52	UofT non-21 FTP server - “possible hack"
17	Nimda related IDS alerts
14	CodeRed related IDS alerts
11	sshd related IDS alerts
3	WEB-IIS cmd.exe access
1	MS-SQL xp_cmdshell - program execution"; warez FTP
2	IDS190/stacheldraht client-check -w/o id
1	IRC and ftp on port 54321

101

Note: These incidents are also included in the statistics on Page 8. In some cases IDS reports include multiple alerts.

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 (July - September)

Number of incidents recorded by type:

- DDoS[1]	2
- Hacking[2]	14
- Harassing e-mail	3
- Malicious Code[3]	49
- Scan/Probe	19
- Spam	116
- Theft/Fraud[4]	1
- Unauthorized Access	0
- Unauthorized Use	0
- IDS-Alerts	90
- Other	48
Total	**342**

Number of internal incidents (originating from campus networks): 273

Number of external incidents[5] (originating from off-campus networks): 62

Number of Other (Origin Unknown): 7

[1] Most of these incidents involved CodeRed & Nimda infected machines. In many cases system administrators hadn't installed available patches.
[2] Incidents that include attempted to actual hacks.
[3] These are mostly SirCam virus incidents. The number of infected machines is higher than the number of incidents as some reports were for multiple machines.
[4] This was a case where copyrighted information was posted on a University server without prior permission from the author.
[5] These include incidents such as Spam as well as incidents involving forged IP numbers.