Security Incidents Report

Reporting Period: January - March 2003

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

Date Prepared: April 2003

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 **January to March 2003**.

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 always 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 January to March of 2003, **270** incidents reports were created.

In all, Computer Security Administration handled approximately **683** e-mail messages during this reporting period (470 in the previous quarter).

There has been an increase of virus/worm related incidents from the previous quarter. CNS needs to increase awareness about the NAV offering.

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.

The Nessus scanner is used for the security sweeps. Full scans are done at least bi-weekly 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.

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.

NESSUS SECURITY SCANS

Scans were conducted on January 23, February 10, February 26, and March 18.

WINDOWS WEAK PASSWORD SCANS
(reports on users in Administrator group only)

Month	# of Hosts	
October	39	
November	15	
January	111	
January	53	Second scan
February	18	
March	15	

In the last three months several critical vulnerabilities were announced.
To check the number of systems susceptible to those vulnerabilities CNS ran additional scans using various tools. These were "incremental" or "delta" scans but as they have been done using different tools their results are not always in the main scan repository but sent directly to the responsible network administrators.

MS-SQL SCANS (buffer overflow, port 1434/udp)

Month	# of Hosts	
February 19	12	
March 12	5	
March 31	1	Rescan of vulnerable March 12 hosts

ORACLE SCANS

Month	# of Hosts
February 24	22
March 11	19

SENDMAIL SCANS

These scan checked only version returned in the sendmail banner. This could be a false positive and it was as the patches don't modify sendmail version. These scans also cover the second sendmail vulnerability announced on March 29.

Month	# of Hosts
March 10	290

MS IIS WebDAV SCAN

This scan checked if WebDAV is enabled (test w/o crashing the service).

Month	# of Hosts
March 26	162

MISCELLANEOUS

We have upgraded to the latest version of the Nessus scanner and made changes in the scan reports format.

ON-DEMAND SCANS

There were 7 "on-demand" scans requested via the web.

Open Relay Scans

The scans were first started in July of 1999.

Scans conducted January 15 to March 31   31
Average number of open relay servers per scan   2

Open Relays By Scan:

January 29	1
January 31	2
February 3	2
February 5	2
February 7	2
February 10	2
February 12	2
February 14	2
February 17	2
February 19	2
February 21	2
February 24	2
February 26	2
February 28	3
March 3	2
March 5	2
March 7	2
March 10	2
March 12	3
March 14	2
March 17	2
March 19	2
March 21	2
March 24	2
March 26	9
March 28	3
March 31	2

There were a total of 9 unique servers that delivered mail during this period.

- One server appeared in 27 of the scans
- One server appeared in 17 of the scans

- One server appeared in 9 of the scans
- One server appeared in 3 of the scans
- Six servers appeared once

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 (October - December)

Number of incidents recorded by type:

Incident Type	Q3 2002	Q4 2002	Q1 2003
DDoS	2	1	2
Hacking[1]	14	6	11
Harassing e-mail	3	6	3
Malicious Code	49	40	69
Scan/Probe	19	68	20
Spam	116	87	98
Theft/Fraud[2]	1	0	2
Unauthorized Access	0	1	0
Unauthorized Use[3]	0	1	5
IDS-Alerts	90	31	15
Other	48	32	45
Total	**342**	**273**	**270**

	Q3 2002	Q4 2002	Q1 2003
Internal incidents (Originating from campus networks)	**273**	**185**	**183**
External incidents[4] (Originating from off-campus networks)	**62**	**88**	**82**
Other incidents (Origin unknown)	**7**	**0**	**5**

---

[1] Incidents that include attempted or actual hacks.
[2] Berne Convention - Demand for Immediate Take Down - Notice of Infringing Activity - Reference#: 1029477]
[3] Unauthorized Distribution of the Copyrighted Motion Picture Entitled Ghost Ship; Unauthorized use of University of Toronto official marks (www.utoronto.us)
[4] These include incidents such as Spam as well as incident444915121s involving forged IP numbers.