Security Incidents Report

Reporting Period: July - September 2003

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

Date Prepared: October 2003

Computer Security Administration Computing & Networking Services University of Toronto

BACKGROUND INFORMATION 3

OVERVIEW 5

NETWORK SCANS..5

VIRUS/WORM INCIDENTS..7

NESSUS SECURITY SCANS...8

WINDOWS WEAK PASSWORD SCANS 8

MS IIS WEBDAV SCAN 8

MISCELLANEOUS..9

SECURITY INCIDENTS STATISTICS...9

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.

Please note the following:

- 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:

1. When a report is received, it is recorded in Remedy.
2. 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).
3. 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.
4. The administrators of any other affected networks are notified. -The incident is tracked and actions taken to resolve the incident are recorded in Remedy.

Overview

This period saw a great deal of activity for University computing resource users and maintainers – especially those using Microsoft products. Two serious bugs associated with the DCOM RPC functionality of Microsoft Windows operating systems were exploited beginning around August 11 with the W32 Blaster worm and, a week later, the Welchia worm. The Blaster worm opened up a backdoor process on the infected host and generated excessive network traffic in trying to spread. In addition, partial host cleaning often caused frequent machine reboots. The Welchia worm was characterized by excessive ICMP traffic used by the worm in its propagation. This traffic appeared to affect core network performance by causing large router CPU utilization. This worm is still infecting many University residence hosts. A number of remedies were implemented by CNS staff to mitigate and/or eliminate the effects of these infections.

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.

VIRUS/WORM INCIDENTS

Description	July – September Incident Count
W32/Blaster • Port 135 used to exploit RPC vulnerability. Port 4444 backdoor opened. Port 135 scanning activity. • Majority of infected hosts were disconnected/repaired within two weeks	500
W32/Welchia • Port 135 used to exploit RPC vulnerability. Port 777 backdoor opened. ICMP echo request scanning activity. • After one month, still 250-300 hosts infected.	500
SoBig.c • Scanning revealed opened proxy servers for SMTP, SOCKS,TELNET,WEB PROXY,FTP and POP3 using port ranges: 1180-1185 and 2280-2285 • Cleared by end of June.	15

In order to notify users and retard the spread of the Blaster worm, CNS took a number of measures: the WTS group generated Windows Messenger notification to infected subnets, port 135 traffic was blocked at department-core boundary points, and application port blocking was permanently implemented at residence-core boundary points. The excessive ICMP traffic generated by Welchia-infected hosts was controlled at department-core boundary points by implementing ICMP threshold filtering to effectively block ICMP from subnets containing many infected hosts. These filters remain in place today. Infected host addresses are detected and published by CNS (http://www.noc.utoronto.ca/net-ops/security.htm to aid department IT staff in their efforts to restore their networks. Also, scans to detect patch status were undertaken regularly to monitor overall vulnerability. See tables below.

Scan Results for RPC DCOM Vulnerability Fixed by Patches MS03-026

Date of Scan	Hosts Patched	Hosts Vulnerable	DCOM Disabled
Aug. 6-7	1136	3955	11
Aug. 13-14	2709	1327	11
Aug.19	3119	625	11
Aug. 25	3101	478	12
Aug. 27	3878	479	15
Sept. 2	5587	710	13
Sept. 8	6771	717	15

Scan Results for RPC DCOM Vulnerability Fixed by Patches MS03-039

Date of Scan	Hosts Patched	Hosts Vulnerable	DCOM Disabled
Sept. 15-16		6079	
Sept. 17		4111	

NESSUS SECURITY SCANS

These scans were run twice per month.

WINDOWS WEAK PASSWORD SCANS

(reports on users in Administrator group only)

Month	Detected Instances
April	44
May	58
June	56
July	112
August	32
September	N/A

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 IIS WebDAV SCAN

This scan checked if WebDAV is vulnerable (test causes host failure if vulnerable).

Date of Scan	Vulnerable Hosts	Notes
April 24	17	including 6 hosts with installed Serv-U FTP servers.
May 14	0	

MISCELLANEOUS

Description	April – June Incident Count
HTTP/SMTP Proxy Servers	14
Other exploits • Backdoor, non-std. port FTP	13
DDoS agents	2

Security Incidents Statistics

Incident Type	Q1 2003	Q2 2003	Q3 2003
Spam • Most incidents originated internally.	98	160	205
Hacking	11	14	16
Scan/probe	20	16	8