Global Information Assurance Certification Paper

Incident Handling Report on the "Denial of Service" Attack On Corporate Mail Servers

Version 1.5b

Hidayath Ullah Khan

May 12th 2001

Table of Contents

1. Executive Summary

On May 1st 2001, at 09:22 hrs, our organization's Help Desk received the first call from corporate users regarding non-receipt of inbound Internet e-mails. On investigation it was found that our corporate Internet mail server "ddditcint1.Tcompany.com", the Microsoft Exchange Server responsible for processing of Internet mail transfers had more than 93,000 e-mail messages building up on the inbound mail queue. The Exchange gateway was not able to cope with these large volumes and crashed at 11:30 hrs on May 1st 2001.

During the course of investigating the incident, it was learnt that an internal employee had inadvertently set off a "denial-of-service" attack on our corporate mail servers. This had resulted in a 6 hours outage on the ddditcint1.Tcompany.com Internet mail server, stopping all inbound mail from the Internet to the whole "Tcompany Group" comprising of about 13,000 employees geographically spread across the globe.

An outage of this magnitude on our corporate mail servers seriously affects the normal functioning of our organization as our company is engaged in a global transportation business and communication is very important. Email is relied heavily to communicate with partners, suppliers, vendors and regional branch offices located in 50 different places across the globe.

In addition to the Internet Mail Exchange Server ddditcint1.Tcompany.com, the following critical Infrastructure Components of our organization also bore the brunt of a self-inflicted "denial-of-service" attack.

Intranet Exchange Server (dddmhex1): Our Intranet Exchange Server "dddmhex1.Tcompany.com" ran out of disk space as nearly 175,000 messages were redirected from ddditcint1.Tcompany.com Internet mail server to a user e-mail account on dddmhex1.Tcompany.com. This resulted in a 14-hour outage on the dddmhex1.Tcompany.com Intranet Exchange Server. Around 400 users whose mail boxes were located on the Intranet Exchange Server were not able to send and receive mail from 15:30 hrs on May 01 2001 to 5:45 hrs May 02 2001 resulting in a significant loss of productivity.

Esafe virus scanning gateway: Esafe gateway crashed, as ddditcint1.Tcompany.com Internet mail server was not available. Esafe gateway is integrated with the corporate Internet mail server and the corporate firewall to perform virus scanning on all inbound emails at their Point of Entry into the network.

Corporate Firewall: There was a degradation of service on the corporate firewall because over 30,000 inbound messages were accumulated on it as it acts as a store and forward server for all inbound emails to the Esafe gateway.

The above Infrastructure breakdown resulted in a significant loss of productivity. The whole "Tcompany Group" of 13,000 employees were not able to receive any inbound Internet mails for a period of 6 hours. Also some very important business users were unable to receive very important e-mails from outside the ddd.Tcompany.com network resulting in a significant loss of revenue. For example, as our company is in a transportation business, it hedges for daily global fuel prices, which are received through

email by our Chief Director, Operations. Since the Internet Mail Server was down this timely information was not received.

I was assigned, to handle this incident (in fact, my very first incident) by our I.T Security Manager and this paper is a result of those efforts as a first time Incident Handler.

The cause of the incident that triggered the "denial of service" attack on our company's critical Infrastructure was determined to be a test script running on the development IIS Web server "dddmiww17.Tcompany.com" located in our company's R&D lab.

The owner/developer of this particular test script Mr. Jake Edward, a software development staff of our company was testing a software module that sends out company Newsletters via email to registered users. To simulate this Newsletters delivery, Jake had written a script that would send messages to a user mail box within the corporate network through the ddditcint1.compay.com mail exchange server. When Jake executed the script on the IIS development web server dddmiww17, it instantaneously generated thousands of messages on the corporate Internet Mail Exchange Server and in the process exhausted all the resources on the Exchange Server thereby rendering it completely useless within minutes.

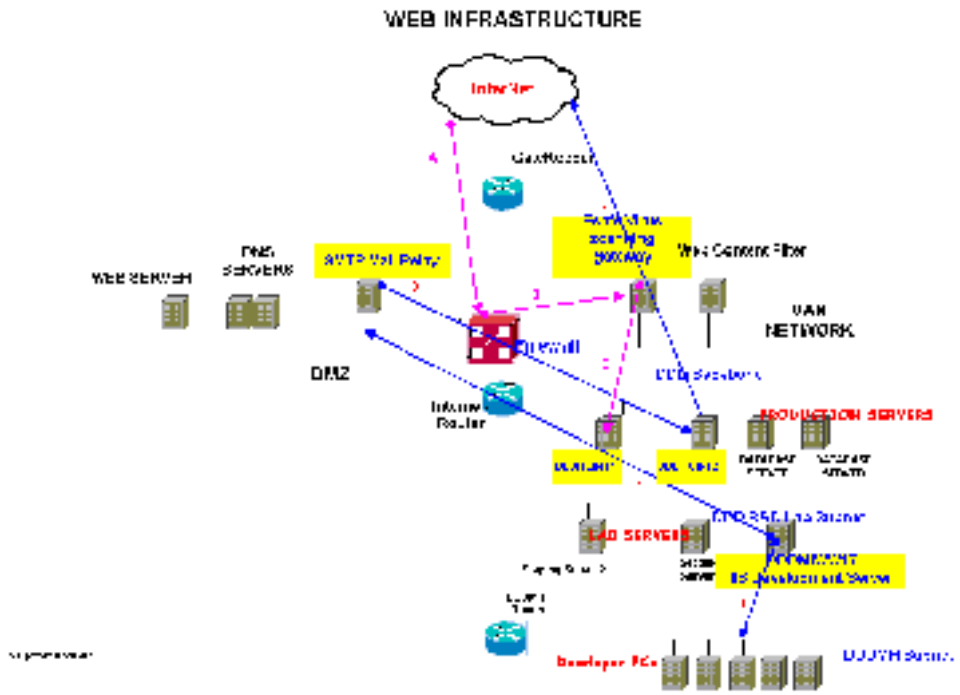
This particular incident also highlighted several serious weaknesses in the following areas of our organization that needs to be assessed and addressed as a matter of urgency.

- No segregation of Development and Production Environments.
- Failure (or lack) of development process and procedures.
- Single points of failure within the Internet e-mail infrastructure.
- Failure of certain development staff to follow testing procedures agreed.

1.1 Our Company's Web Infrastructure Background:

Our company mostly uses in -house developed softw are for its business activities. The software developers in our company develop and test their code on development servers located in the company's R&D development Lab before promoting it on the production servers.
As part of their development and testing process, the developers needed the ability to send and receive Internet emails from the development servers. To support this activity a smtp server "smtp96" running on Windows NT version 4.0 was commissioned in the DMZ area of our network to act as a Mail Relay Server. The Mail Relay Server "smtp96" was configured to send outbound mails through "ddditcint2.Tcompany.com" and receive inbound Internet mails through "ddditcint1.compay.com" The corporate firewall was configured to allow email transfers from the IIS development server "dddmiww17.Tcompany.com" to "smtp96.Tcompany.com" Mail Relay server.

The diagram below illustrates the above web infrastructure scenario. The arrows indicate the outbound and inbound mail flow path.



What follows is a description of the Incident, our organization's security preparations prior to the Incident, the Incident Identification and Containment and finally finishes with some lessons learned and recommendations to prevent such incidents from occurring again.

I tried to closely follow the recommended Incident Handling practices by dividing the handling process in to six phases –

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

2. Phase – 1: Preparation

After having barely completed the online Incident Handling and Hacker Exploits course, I had just begun to appraise our newly appointed IT Security Manager "Ro" about the enormous benefits of preparing ourselves for an incident cold when this incident suddenly occurred. Ro had just joined our organization and until then we had had no proper security practices or policies in place. Ro had created some security policies and was still in the process of reviewing it with the Management when this incident occurred. In other words, we were not yet "prepared" with policies, skilled people & other resources to respond to an Incident.
When Ro was informed about the incident from the Senior Manager, he called me in his office and informed me that it was now time to put into practice whatever I've learned in the online Incident Handling course. He assigned me as the primary Incident Handler for this incident because I was the only person in the organization with some knowledge about Incident Handling.
Armed with the little knowledge I had acquired from the SANS Online Incident Handling Course, I set out to handle the incident as best as I could. The very thought of "Incident handling" made me feel tense and excited. I then remembered the wise words on the Emergency Action Plan in the Incident Handling curriculum to remain calm. I started breathing deeply, grabbed a notepad and the incident handling pre-printed forms that came along with the Incident Handling Step by Step guide and left to scene of the incident – our R&D lab.

3. Phase – 2: Identification

Identification involves determining whether or not an incident has occurred, and if one has occurred, determining the nature of the incident. Identification normally begins after someone has noticed an anomaly in a system or network. This phase also includes informing and soliciting help from other people who can help understand and solve the problem.

While leaving to the scene of the Incident, I called our Help Desk, the Messaging Manager and a few others to provide me with more information about the incident. I also requested for a stand-by resource in case I need some help.

The table below illustrates Who, How & When the Incident was identified.

Identification Table

Date/Time	By Who	Comments
May01,2001, 9:22hrs	Help Desk	Help Desk receives call from users inquiring about no inbound emails
May01,2001, 10:30hrs	Messaging Team / Peter	A check on the Exchange Server logs indicates that approximately 93,000 messages were building up on the ddditcint1.Tcompany internet mail server. All mails were originating from dddmiww17.Tcompany.com web development server
May01,2001, 11:30hrs	R&D/Samuel	Analysis of IIS and SMTP Logs on dddmiww17.Tcompany.com system indicate thousands of messages have been transferred to dddmiww96.Tcompany.com system from the dddmiww1 7 system
May01,200, 13:45hrs	R&D/Samuel	SMTP Logs on dddmiww96.Tcompany.com system indicate that all the mails have jake.edward@Tcompany.com as the sender and skycgoenews@Tcompany.com as the recipient.
May01,2001, 15:30hrs	Messaging Team	Exchange Server dddmhex1 runs out of disk space.

4. Phase – 3: Containment

The goal of the containment phase is to limit the scope and magnitude of an incident, to keep the incident from getting worse.

Before summoning me, Ro had already instructed the Lab assistant to contain the incident by performing a controlled shutdown of the suspect machine from which the email messages were being propagated. By the time I reached t he scene, dddmiww17 system was already down. I then took dddmiww17 system in to my custody, changed the administrator password and unplugged it from the network. The messaging team had by then stopped the Internet mail connector service running on ddditcin t1.tcompany.com Microsoft Exchange server to stop processing of the pending mail queues.
I could not locate any parallel port tape drives to take a standalone backup of the dddmiww17 system. Moreover, critical forensic system evidence was already destroye d, as dddmiww17 was shutdown soon after learning about the incident in an attempt to contain further damage to the corporate network.

The table below illustrates the actions performed by the various teams to contain the Incident.

Containment Table

Date/Time	By Who	Action	Comments
May01,2001, 11:45hrs	R&D Lab/Samuel	Shutdown of dddmiww17.Tcompany.com	IT Security Manager, Ro issues instructions to perform a controlled shutdown of dddmiww17.Tcompany.com
May01,2001, 12:00hrs	Messaging Team	Jake Edward & skycgoe emails accounts are blocked	to prevent any emails coming in from "jake.edward@Tcompany.com" and "skycgoenews@Tcompany.com"
May01,2001, 12:00hrs	Messaging Team	Stopped Internet Mail Connector service on ddditcint1.Tcompany.com	to stop processin g of queues on the Internet Server
May01,2001, 14:00hrs	IT Security Group//KK	Dddmiww17.Tcompany.com system taken in to custody	Unplugged the network cable and disconnected dddmiww17.Tcompany.com from the network
May01,2001, 14:00hrs	IT Security Group//KK	Attempt to take a backup of dddmiww17.Tcompany.com	**Could not locate any parallel port tape drives to take a standalone backup of the dddmiww17 system. Moreover, critical forensic system evidence was already destroyed as dddmiww17 was shutdown by the lab assistant soon after learning about the incident,**
May01,2001, 15:00hrs	IT Security Group/KK	IIS & SMTP logs analysis	Start of investigation

5. Phase – 4: Eradication

The goal of the eradication ph ase is to make sure the problem is eliminated and the avenue of entry is closed off.

The following steps were carried out:

- Incident Analysis - to determine the cause and symptoms of the incident
- Improved defenses by disabling some service on the suspect system
- Vulnerability analysis of the script.

Incident Analysis:

A detailed analysis of the incident was done by correlating the logs on the IIS development system 'dmiww17', Mail Relay Server 'smtp96' and by speaking to some R&D Lab support staff who w ere involved in a similar incident earlier.
The following chronological events leading to the unavailability of ddditcint1 & dddmhex1 mail systems are unfolded below -

- On April 14th 2001, Mr. Jake Edward, Software Engineer from the Software development team runs the test script "cdomail.asp" on dddmiww17. The objective of this testing was to confirm the ability of the system to send the news mails automatically to multiple Internet e -mail addresses.

- The recipient email address specified on this script was Meta Blomkvist, Projects Controller, Software development Team. The script when executed generated nearly 2000 email messages within a few minutes in Meta Blomkvist's personal mailbox on dddmhex1 (Production mail server). Jake Edward aborts the script and requests John a temp staff in R&D Lab over the phone to clear the pending mail queues on dddmiww17 system. Jake also calls Peter from the Messaging team and informs him about the huge mails being generated on Meta Blomkvist's mailbox. Peter strictly in structs Jake not to test scripts on production mailboxes and creates a test mailbox called skycgoenews@Tcompany.com . Peter also informs Jake not to perform any future testing without obtaining a prior consent from the Messaging Team.

- On April 16th 09:30 hrs, the same script "cdomail.asp" is executed again by Mr. Edward with the destination address of skycgoenews@Tcompany.com . The script generates 5000 email messag es to skycogenews account created by the Messaging Team. The Software development team member realizing that the script was again generating a lot of messages calls John over the phone to stop the smtp service running on the dddmiww17 system and also reque sts him to clear the messages from the email queue. John stops the smtp service, clears the mail queues and reboots the dddmiww17 machine as per Jake's instructions. NOTE: The messaging team was not informed of this test as agreed on the 14 th April.

- On April 16th 09:50 hrs, Mr. Jake Edward runs the script again for the 3 rd time resulting in the generation of over 30,000 messages within few minutes destined for the skycogenews mailbox via the internet mail gateway. Jake calls John again over the phone to s top the smtp service running on dddmiww17. This time John only stops the smtp service but does not clears the mail queue on dddmiww17 system, as he was not instructed to do so.

- The event logs on the dddmiww17 system indicate no system reboots between Apri l 16th and April 30th 2001

- On April 30th 15:30 hrs, a sudden power outage of a few seconds brings down all the R&D Lab servers.

- On May 01st around 8:30 hrs, the dddmiww17 system is brought back online by the Lab assistants. The "smtp service" which was turned off by John on the 16 th April is started automatically by default as the system comes online. The smtp service then starts sending out all the mails that were queued and not cleared on the 16 th April 2001. This resulted in about 93,000 e -mails being sent via the Internet mail gateway (ddditcint1) destined for Mr. Edward's mailbox and the skycargo test mailbox. The volume of inbound mails to the ddditcint1 server caused it to crash due to the sheer load. This stopped all inbound Internet mail for t he TCOMPANY Group.

- Since the internet mail server "ddditcint1" was down, the Mail Relay server "smtp96" was trying to redirect all the undelivered messages to the Microsoft Exchange System

'dddmhex1' located on a different subnet where the software development Team member Mr. Jake Edward's mailbox was hosted. Consequently, on May 01st around 15:30 hrs, the dddmhex1 Exchange Server ran out of disk space. This prevented all the users from sending and receiving mail for 14 hours whose mailbox was hosted on the 'dddmhex1' mail exchange server.

The table below illustrates the eradication steps carried out.

Date/Time	By Who	Action	Comments
May01,2001, 15:00hrs	IT Security/KK	Analysis of IIS, SMTP logs on dddmiww17 system	Indicated that cdomail.asp script was executed on the April 16th 2001
May01,2001, 15:00hrs	IT Security Group/KK	Stopped SMTP Service on dddmiww17.tcompany.com	Complete eradication of the incident by making sure that the smtp mail forwarding is disabled on the dddmiww17 IIS development server.
May01,2001, 17:00hrs	IT Security/KK	Attempt to do a vulnerability analysis of the asp script on dddmiww17	Script was not found **Please see note1**
May01,2001, 18:00hrs	IT Security/KK	Attempt to restore the original script on dddmiww17	**Please see note2**

Note1: I searched the dddmiww17 IIS development system for the script in order to analyze it further. But I couldn't locate the script ; Jake had deleted the script from dddmiww17 on April 16th itself. Initially he denied ever deleting it but after a lot or persuasion he confessed at having deleted it on the 16th. However, it was not clear if the script was run again on May 01 2001, as system forensics like processes, temp files were deleted from the system as dddmiww17 was shutdown by R&D staff soon after learning about the incident, in an attempt to contain further damage to the mail servers.

Note2: As I was not able to locate the script on dddmiww17 on May01, I attempted to restore the May 16th backup to analyze the script further. But as all the development systems at R&D Lab are backed up on a daily basis and the tapes rotated weekly, the crucial 16th April tape data was overwritten by new data. Hence there was no evidence of the original script.

To completely eradicate the problem and prevent it from reoccurring again, I turned off the smtp mail forwarding service on dddmiww17. I also made sure that the rouge script cdomail.asp was not present on the system.

6. Phase – 5: Recovery

In the Recovery phase, the goal is to return the system to a fully op erational status.

The following actions were performed to restore the mail systems back to normal conditions –

- Internet mail connector service was restarted on the dddintcint1 system and the system released for production.
- Performed some house keeping ope rations like deleting directories and clearing logs to create more disk space on dddmhex1 system.

The table below illustrates the steps taken to recover the ddditcint1 & dddmhex1 mail systems.

Date/Time	By Who	Action	Comments
May01,2001, 15:30 hrs	Messaging Team	Deleted some directories on the dddmhex1 Server to recover space. 158MB recovered	DDDMHEX1 Server ran out of disk space because the script was populating Jake Edward's mailbox on DDDMHEX1.Tcompany.com mail server
May01,2001, 15:40hrs	Messaging Team	Restart the Internet Mail connector on ddditcint1.Tcompany.com	Internet Mail Server ddditcint1.Tcompany.com was restarted and the system was released to production.
May01,2001, 17:45 hrs	Messaging Team	Deleted "Jake Edward's mailbox which had grown upto 982 megabytes	The dddmhex1.Tcompany.com ran out of disk space again
May01,2001, 17:45 hrs	Messaging Team	Moved the following mailboxes to the Site A Exchange Server: DIT,	To prevent disruption of email services to Director, IT
May01,2001, 21:45hrs	USG/SSS	Installation of an additional Hard Disk on the DDDMHEX1 Server	This would bring back the dddmhex1 server back to normal.
May01,2001, 22:00hrs	Messaging Team	Disabled the "skycgoenews" mailbox by removing the X.400 and SMTP address entries	To preserve space on the dddmhex1 server.

7. Phase – 6: Lessons Learned

This incident has highlighted several significant risks and exposures in the following areas of our organization:

- Development and Production activities on the same network. Development activities caused an outage for production users worldwide.
- Inadequate SDLC process. There is no evidence of the development teams following any agreed process for developing, system testing and user testing new applications. As can be seen in this case, even a user mailbox was used for the testing.
- Development staff failed to follow the instructions agreed with the messaging team for performing such tests. The test -run by the developer on 16th April was not scheduled with the messaging team. Such communication could have avoided this incident.
- Inadequate physical security of the Lab.
- Inadequate logical security controls on the development system. A virtual domain had been configured on the system giving development staff full control of certain directories and services.
- Esafe virus scanning gateway a single point of failure.
- No Emergency Action Plan in place with agreed responses, escalation etc.
- Single domain architecture combines production and test servers and all associated traffic over the same network.
- Additionally, the developers in question did not seem to appreciate the extent or seriousness of the outage they caused and were not very co-operative during the investigation.

8. Incident Impact:

- Denial of service on the Production Internet Mail Server – No inbound emails, users world-wide affected for 6 hours
- Exchange System runs out of disk space – users were not able to send and receive mail for 14 hours.
- Esafe virus scanning gateway: Esafe gateway responsible for virus scanning of all inbound emails crashed as ddditcint1 Internet mail server was not available.

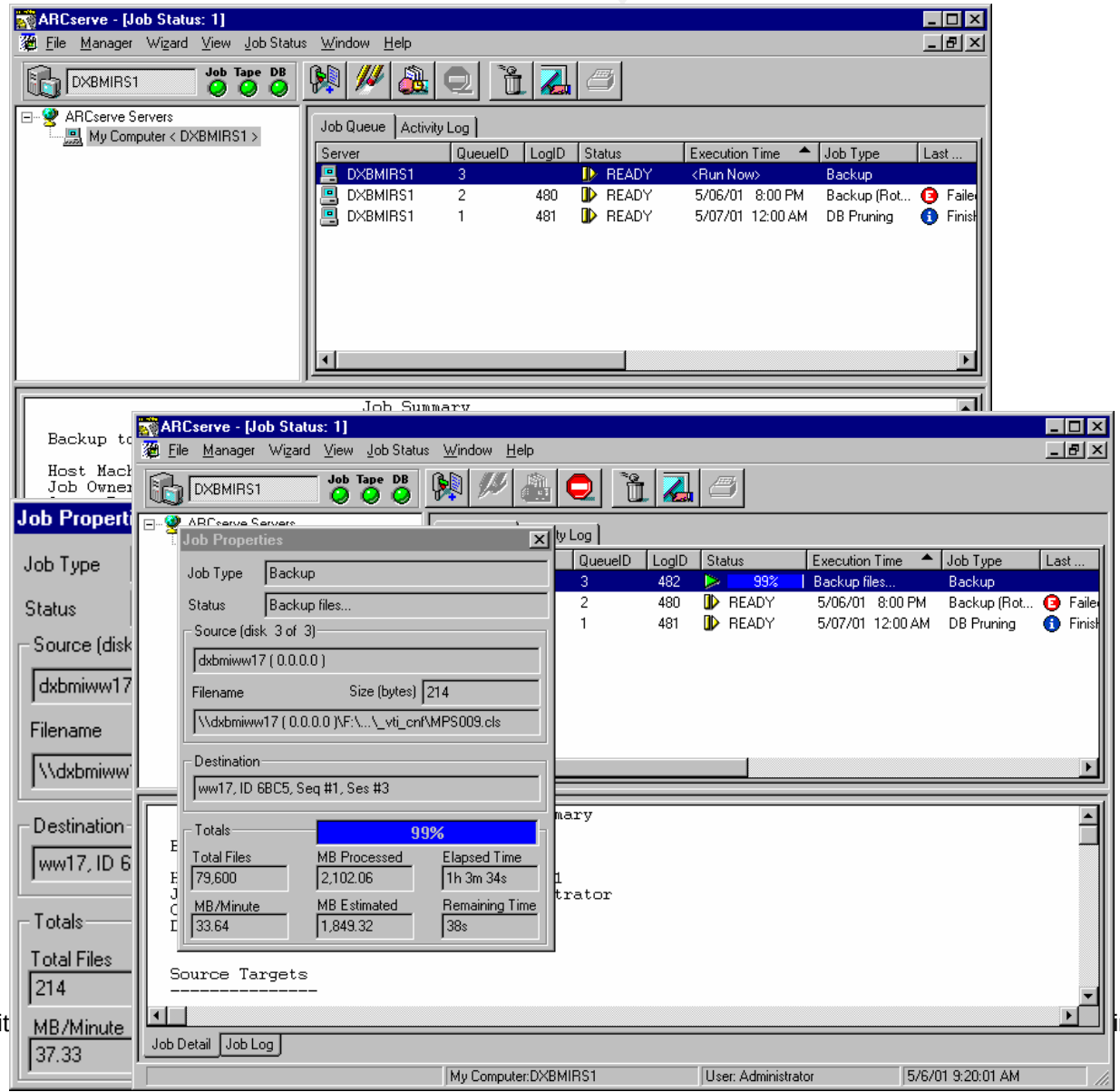
- Corporate Firewall: There was a degradation of performance on the corporate firewall and it was on the verge of collapsing as more than 30,000 inbound messages were accum ulated on the firewall as it acts as a store and forward server for all inbound emails to the virus scanning gateway.

- Business users unable to receive important e -mail from outside the company network in a timely manner (e.g. daily fuel prices received b y Chief Director).

- Productivity impact as scheduled work had to be postponed while the incident was investigated. Disruption for all development and support staff.

9. Backups:

Before releasing the IIS development system for development, I intended to per form a full backup of 'dddmiww17' to preserve any system evidence in case it was required later. As we did not had any parallel port tape drives to perform a standalone backup of dddmiww17, I decided to use Arc Serve Network Backup after office hours. Afte r making sure that no users or developers were around, I reconnected dddmiww17 system back to network and checked the event logs to make sure no one was trying to connect to the system. I then initiated a full network backup of ddmiww17 system.



10. Chain of Custody:

After making sure that the tape was “write -protected”, I handed the backup tape to our IT Security Manager, who in turn handed it over to IT Operations Manager for safe keeping in the data center fireproof safe. We then filled a chain of custody form clearly describing the contents of tape, owner, date & time of backup and a brief summary of the incident.

11. Recommendations:

- Logical separation of Production and Development Network
- Complete review of change management process and practices
- Review of the backup strategy
- Review of all developer system access privileges
- Enforce physical access controls on the R&D Lab via swipe card.
- Development of emergency response procedures
- Enforce Security Auditing on all systems

12. References:

Malisow, Ben. “Moment's Notice: The Immediate Steps of Incident Handling”. Friday, July 7, 2000
URL: http://www.securityfocus.com/

Fordham, Doug. “Intelligence Preparation of the Battlefield”. Monday, June 19, 2000
URL: http://www.securityfocus.com/

Malisow, Ben. “Personal Interface: The Relationship between Users and Security Personnel in the Modern Environment”. Monday, April 27, 2000
URL: http://www.securityfocus.com/

Wright, Timothy. “An Introduction to the Field Guide for Investigating Computer Crime”. Monday, April 17, 2000
URL: http://www.securityfocus.com/

Allgeier, Michael. “Digital Media Forensics”. Monday, May 8, 2000
URL: http://www.securityfocus.com/

Spitzner, Lance. “Know Your Enemy: A Forensic Analysis”. Tuesday, May 23, 2000
URL: http://project.honeynet.org/

Ferrel, Robert. “Chasing the Wind”. Sunday, September 17, 2000
URL: http://www.securityfocus.com/