Examples

The following examples show some of the types of information that are available to the victims of computer misuse. Real examples have been used with names and addresses modified to protect the sites involved. These are typical of the evidence that may be sent to a site to complain about the activities of its users. In each case the receiving site will need to use additional logs relating to its clients and intermediaries to understand and investigate the origin of the misuse.

Attempted Break-in

The following entries were recorded by syslog on a UNIX® system called victim, whose clock is known to be synchronised to a reliable UK time source (see section 6.2):

```
Jul  4 19:08:11 4Q: victim telnetd[338556]: connection from
attacker.example.ac.uk Jul  4 19:08:12 0F: victim
telnetd[338556]: ignored attempt to setenv(_RLD, ^?D^X^\
^?D^X^^

^D^P^?^?$^B^Cs#^?^B^T#d~^H#e~^P/d~^P/`~^T#`~^O^C^?^?L/bin/

sh%32614c%11$hn%86

000c%12$hn)
```

This shows an apparently normal telnet connection from the host **attacker.example.ac.uk**, during which the attacker attempts to overflow a buffer in the telnet server program. This is clearly an attack, whose intent is to obtain a command shell **(/bin/sh**) with root privilege, so the victim site would expect Example to investigate. Provided **attacker.example.ac.uk** is an end-user machine, this should simply be a case of identifying the person who was logged on to that machine at 19:08 on 4 July. If attacker is an intermediary, for example a network address translation (NAT) system, then its logs will need to be used to identify the internal host that was the source of the activity. In practice it is most common for this type of attack to come from a host that has itself been compromised, often using the same attack, so the file system and logs on attacker will also need to be checked for signs of malicious activity. This also means that times and logs on the attacking machine may have been modified so user records from a central authentication server (if available) may be a more reliable source.

It is worth noting that **victim** was one of a number of similar machines in its department that were subject to this attack. **victim** had been patched, so the attack on it was unsuccessful. The other machines were compromised, and no trace of the attack was left in their syslog files.

Inappropriate E-mail

A complaint was received from a Microsoft network subscriber who had received an offensive e-mail:

```
From: heidi32396@example.ac.uk <heidi32396@example.ac.uk>

To: user@msn.com <user@msn.com>

Subject: Teens & Hot Horny Housewives
```

This was already suspicious as the username given in the From field of the e-mail is not of a form used by Example and there is no user of that name. The full headers from the e-mail were obtained from the complainant, and showed clearly that the e-mail had not originated from a Janet site:

```
Received: from cpimssmtpa02.msn.com - 207.46.181.107 by email.msn.

com with

Microsoft SMTPSVC;

   Fri, 11 May 2001 13:09:34 -0700

Received: from njkkkkkkk.com ([38.31.27.7]) by
cpimssmtpa02.msn.com with

Microsoft SMTPSVC(5.0.2195.3225);

   Fri, 11 May 2001 12:56:53 -0700

Message-ID: <NApRVdL7bndr-.YGar-xZdAAl8Fi2SQJtihM@njkkkkkkk.com>

From: heidi32396@example.ac.uk <heidi32396@example.ac.uk>

Bcc:

To: user@msn.com <user@msn.com>

Subject: Teens & Hot Horny Housewives

Date: Sun, 05 Mar 2000 20:34:33 -0400 (EDT)

MIME-Version: 1.0

Content-Type: text/plain; charset="US-ASCII"

Content-Transfer-Encoding: 7bit

Return-Path: heidi32396@example.ac.uk
```

The Received headers created within the msn.com domain indicate that the message in fact originated from a customer of an American ISP, and that references to Example had been forged to conceal the true origin of the message. The logfiles of the mail server at Example further confirmed that no message had been sent to the recipient e-mail address from that site.

The message may have been forged by the ISP's customer, or may have been inserted into the Internet through a badly configured proxy or other system at the customer site. Both

techniques are all too common ways to generate volume advertising by abusing services provided and paid for by others.

Abuse of Webmail Service

A customer of an international ISP received an offensive e-mail from an address at **hotmail.com**. Hotmail is a webmail gateway, so is effectively an intermediary. Like many other webmail systems, Hotmail adds headers to the e-mail it sends that include the IP address of the host that submitted the web request to Hotmail that caused it to generate the message. On inspection of the full headers of the offensive mail message the following information was found.

```
Received: from mail pickup service by hotmail.com with Microsoft
SMTPSVC; Thu, 12 Apr 2001 08:12:26 -0800

Received: from 192.251.0.8 by lw3fd.law3.hotmail.msn.com with
HTTP;  Thu, 12 Apr 2001 16:12:21 GMT

X-Originating-IP: [192.251.0.8]

Date: Sun, 1 Apr 2001 10:00:00
```

The X-Originating-IP header and lines above it were written by Hotmail and are usually reliable; note that the Date header has been forged by the creator of the offensive mail. Including reliable information in the outgoing message means that in most cases it will not be necessary to search through the logs on the Hotmail intermediary. However, these logs should still be kept, as there have been attempts to forge or conceal this X-Originating-IP information.

The IP address **`192.251.0.8`** belongs to a site cache, so the logs on this cache must be checked to determine which local host was responsible for the request. This involved searching for the Hotmail host named in the last of the received lines: **`lw3fd.law3.hotmail.msn.com`**. The following entry was found, but note that there is a 10 second difference in the time stamps. In this case the correct sender was identified but even this time difference, which was due to a failure to synchronise the system clocks to an international standard, could have prevented or cast doubt on the identification of the offender.

```
Thu Apr 12 16:12:31 2001 6913 babel.comp.example.ac.uk
TCP_MISS/200 12339 POST http://lw3fd.law3.hotmail.msn.com/cgi-
bin/premail/4284 - DIRECT/209.185.240.250 text/html
```

`babel.comp.example.ac.uk` is a single-user workstation and its login records showed the identity of the account that was logged in at the time of the offensive posting.

Denial of Service Attack with a Web Server Intermediary

The site

intermediary.ac.uk

observed an unusually large traffic load on its link to the JANET network. At the same time the web server of `victim.com` suffered a denial of service attack, receiving a large number of packets from **`www.intermediary.ac.uk`**. On further investigation, the following request

was found in the web logfile on **www.intermediary.ac.uk**.

```
   2001-06-28 09:34:37

webcache.attacker.ac.uk - www.intermediary.ac.uk

80 GET /scripts/../../winnt/system32/cmd.exe /c+ping+-v+ping%20-

   n+2000+-l+65500+-w+0+www.victim.com 132 502
```

This indicates that the web server received a request from a host called **webcache.attacker.ac.uk**. It is a reasonable guess that this host is itself a proxy. The filename requested contains a series of **'../**' entries which attempt to move the program out of the initial '**/scripts**' directory and indeed out of the area normally containing web scripts or files. This should not be valid and should be rejected as an illegal request, but the web server program had a well known bug, known as a directory-traversal vulnerability, which let it accept and service requests of this type rather than returning an error message. The directory traversal is used to move to the Windows system directory and to run the 'ping' command with parameters to make it generate 2000 packets, each 64K bytes in size, as fast as possible. These caused both the unusual traffic flow and the denial of service attack.

Because the web server logs are available it is possible to identify the system **webcache.attacker.ac.uk** from which the request came. However, as this system is itself a proxy, the attack must be traced back by checking the logs on that proxy for a request made to **www.intermediary.ac.uk** at that time, and containing the same request string. The cache logs should identify the client machine responsible and from its login records the offending user can be found.

This final example illustrates the range of logs that can often be needed to trace activity back to its source. Not all the computers through which an attack passes will themselves be compromised; they may be performing quite correctly or just offering a service that has been used in an unauthorised way. Indeed, even though the web server in this case could have been broken in to using the same vulnerability, it was not necessary to do this to make it participate in a denial of service attack that was disruptive both to the target and to the intermediary site.
