



Guidance Notes

Investigating a
denial-of-service
attack

Contents

1	Introduction.....	5
2	Network infrastructure.....	5
3	The network monitor.....	6
4	What we saw.....	6
5	Aftermath.....	7
6	Contact information.....	8
7	References.....	8

Investigating a denial-of-service attack

This paper has been contributed by a JANET customer site, and records their experiences in investigating a denial-of-service attack committed using hosts at their site. We are very grateful to them for allowing us to publish this information and hope that it will be useful to others.

1 Introduction

During the summer of 2000 our institution (a UK university) was identified as a participant in a Distributed Denial-of-Service (DDoS) attack against a number of foreign sites. This paper briefly summarises the technique we used to trace the machines involved - a task often complicated by the use of IP spoofing [1] to disguise the actual source of an attack.

The incident began with a call from a user concerned about a sudden increase in the number of events recorded by his personal firewall software [2]. The logs indicated several periods of intense network activity during the previous night, apparently involving multiple local hosts. Unfortunately, by the time the report was received, traffic levels had returned to normal leaving no indication of the likely cause.

Within a few hours more reports began to arrive from remote sites that had been on the receiving end of a denial-of-service attack originating from the departmental network where our user was located.

2 Network infrastructure

The university network is based on a Gigabit Ethernet backbone, linking together departmental Local Area Networks (LANs) which typically deliver switched 10/100Mbit/s to the desktop. The network is shown diagrammatically in Figure 1.

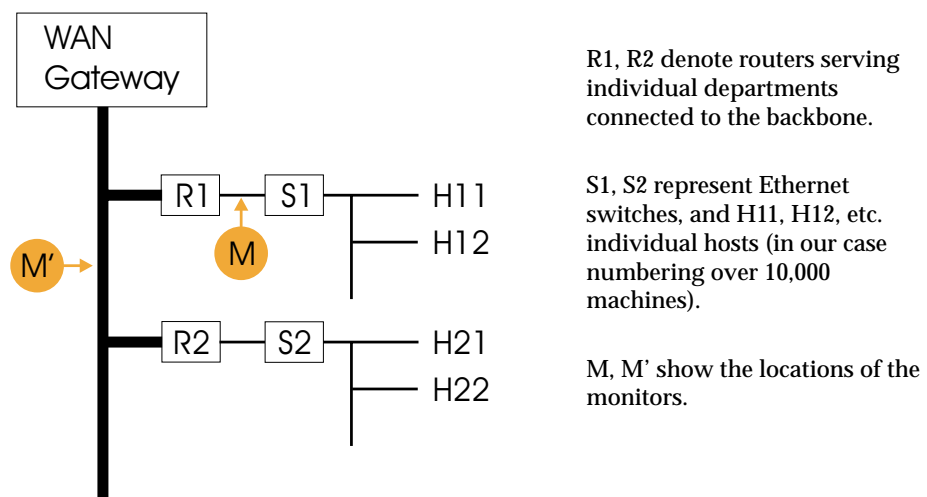


Figure 1: Schematic of the university network

We primarily use Cisco routers and switches, and routinely make use of the comprehensive logging facilities found in most of their equipment. On this occasion, however, we had little idea of the characteristics of the problem traffic, nor when it might occur again. Knowing only which departmental LAN contained the attacking systems, we chose to use a separate network monitor that could be configured to look for a wider range of anomalous behaviour, if necessary under programmatic control. But our first problem was how to monitor traffic in a switched environment.

Two options are normally available:

- use diagnostic facilities available in the switch to mirror all traffic to a single port, to which the monitor can be attached;
- connect a hub between the router interface and the switch, and then attach the monitor to a spare hub port.

Either approach can have an impact on network performance, and may cause packet loss. In the circumstances however (compromised hosts on the network), this is likely to be a relatively minor concern in the short term.

We went for a slight variation on the first option. Cisco offers a Remote Switched Port ANalyser (RSPAN) feature that can tunnel mirrored traffic back through a number of intermediate switches and routers to a convenient location. In our case, leaving a monitor permanently sited in the machine room is much preferable to moving it around the university. Logically, this is still equivalent to attaching the monitor to point M in Figure 1.

3 The network monitor

Our monitor is a Linux system running the Snort lightweight intrusion detection system [3]. Demands on hardware are not very high: we use a redundant Pentium 133-based system with two 10/100Mbit/s network interface cards, 128MB memory and 4GB disk space. This allows us to use one interface to access the console, while the other is dedicated to the RSPAN traffic. It is configured with a minimum number of services running and no user accounts [4].

Snort is basically a packet sniffer for which a library of network attack signatures is available. It uses signatures in much the same way that most anti-virus software uses them, to recognise patterns in viral code. Snort is not really stateful, and normally analyses packets independently of each other. Preprocessor plugins can be used to extend functionality, for example to detect port scans.

Suspecting that IP spoofing might be involved, we want to preserve layer 2 addressing information. This is often critical in identifying the true source of spoofed traffic, as most spoofing occurs at layer 3 (IP), rather than at layer 2 (the MAC address). To this end, we can invoke Snort with the following command line options:

```
[root@monitor]# snort -D -N -e -i eth1 -c ./08292k.rules -l ./logs
```

The meanings of the options are as follows:

-D	run in background (as a daemon)
-N	do not attempt to log packet payload
-e	record layer 2 information
-i eth1	read packets from interface eth1
-c ./08292k.rules	name of file containing attack signatures
-l ./logs	write log files to this directory

4 What we saw

We left the monitor in place for two days, until our log file began to grow rapidly indicating a new attack in progress. The following entries are typical of what was observed:

```
[**] IDS253 - DDoS shaft synflood outgoing [**]
06/12-14:30:46.599036 8:0:20:1B:22:A9 -> 0:D0:D3:56:D1:30 type:0x800
len:0x3C
98.76.54.111:1008 -> 12.34.56.78:6666 TCP TTL:30 TOS:0x0 ID:59926 DF
**S***** Seq: 0x28374839 Ack: 0x3E0D641F Win: 0xFFFF

[**] IDS253 - DDoS shaft synflood outgoing [**]
06/12-14:30:46.602703 8:0:20:1B:22:A9 -> 0:D0:D3:56:D1:30 type:0x800
len:0x3C
98.76.54.93:1020 -> 22.44.66.88:6667 TCP TTL:30 TOS:0x0 ID:59936 DF
**S***** Seq: 0x28374839 Ack: 0x3E0D641F Win: 0xFFFF
```

```
[**] IDS253 - DDoS shaft synflood outgoing [**]
06/12-14:30:46.769474 8:0:20:1B:22:A9 -> 0:D0:D3:56:D1:30 type:0x800
len:0x3C
98.76.54.224:1009 -> 12.34.56.78:6667 TCP TTL:30 TOS:0x0 ID:59940 DF
**S***** Seq: 0x28374839 Ack: 0x3E0D641F Win: 0xFFFF
```

Each entry corresponds to a packet matched against an attack signature. We have three packets, sourced apparently from three different hosts on our network (98.76.54.111, 98.76.54.93, 98.76.54.224) and targeted at two machines (12.34.56.78 and 22.44.66.88). Several characteristics recorded by Snort are interesting, but most especially the layer 2 (MAC) addresses. As we would expect, the destination MAC address (0:D0:D3:56:D1:30) is in each case that of our router - the gateway to the rest of our network and, ultimately, the outside world. But we also see that the source MAC addresses are all the same (8:0:20:1B:22:A9). Although the IP addresses indicate the traffic is coming from three different machines, the layer 2 information shows they in fact originate from the same ethernet card.

This uniquely identifies the real source of the attack. If you keep records of system hardware addresses, associating the card with a named system is then trivial. If records aren't available, broadcast pings on the network followed by inspection of the arp cache can help. For example, on an NT workstation connected to the departmental LAN:

```
C:\> ping 98.76.54.255
C:\> arp -a

Interface: 98.76.54.101 on Interface 2

Internet Address      Physical Address      Type
98.76.54.2            08-00-xx-xx-xx-xx    dynamic
98.76.54.11           00-30-xx-xx-xx-xx    dynamic
98.76.54.22           00-60-xx-xx-xx-xx    dynamic
98.76.54.24           08-00-xx-xx-xx-xx    dynamic
98.76.54.25           08-00-20-1b-22-a9    dynamic
98.76.54.30           00-60-xx-xx-xx-xx    dynamic
98.76.54.31           08-00-xx-xx-xx-xx    dynamic
98.76.54.32           00-30-xx-xx-xx-xx    dynamic
```

Otherwise it is a matter of checking machines by hand.

In our case, a detailed examination of host 98.76.54.25 (a Sun Solaris system) revealed the presence of several trojan versions of system binaries (including /bin/login and netstat). Sun's fingerprint database [5] was particularly helpful here. Linux users might use rpm's verify capability to a similar end, assuming that the rpm database has not itself been tampered with.

5 Aftermath

In this particular incident, the initial tip-off led directly to the departmental network containing the compromised hosts. This information is not always so readily available, since IP spoofing can also be used to simulate traffic from machines on many different networks. Such a situation could be handled by repositioning the network monitor on the backbone (at M' in the diagram, for example), and again examining the source MAC addresses of attack packets (but note that performance is likely to be a concern, with monitors dropping traffic at gigabit speeds). In this case, the MAC address will identify the router (R1, R2 in our diagram), and hence the sub-network from which the traffic originates. It is, however, much better to take a preventive approach and use egress filters on the departmental routers to prevent spoofing of non-local traffic [6].

We had some further success using the Nessus remote security scanner [7], which can detect a number of inactive DDoS agents, handlers and other backdoors. Several were located and steps taken to secure them.

Although this description relates to the technical aspects of responding to a particular incident, it is worth emphasising that these steps are primarily reactive in nature. The greatest challenge facing our institution now is to develop our organisational controls and improve awareness of security issues. Only by tackling the much broader problem can we hope to see the frequency of such events significantly reduced.

6 Contact information

Names and addresses have been altered. Individuals wishing to contact us for further information are invited to do so via JANET-CERT (cert@cert.ja.net).

7 References

- [1] Microsoft TechNet - Source Address Spoofing
<http://www.microsoft.com/technet/security/sourcead.asp>
 - [2] ZoneAlarm
<http://www.zonelabs.com/>
 - [3] Snort - the Lightweight Network Intrusion Detection System
<http://www.snort.org/>
 - [4] Armoring Linux
<http://www.enteract.com/~lspitz/linux.html>
 - [5] SunSolve: The Solaris Fingerprint Database
<http://sunsolve.sun.com/pub-cgi/show.pl?target=content/content7>
 - [6] SANS Institute: Information Security Reading Room
What is an Egress Filter and How Can I Implement it?
<http://www.sans.org/infosecFAQ/egress.htm>
 - [7] The Nessus Project
<http://www.nessus.lug.org.uk/>
- A current list of backdoors recognised by Nessus can be found at
<http://cgi.nessus.org/plugins/dump.php3?family=Backdoors>.

Tell us what you think

Guidance Notes are produced and published by UKERNA for use within the JANET Community. We welcome your comments on all aspects of this document and on any other UKERNA publication. Please direct feedback to JANET Customer Service, at the address below, or e-mail us directly at:

documentation@ukerna.ac.uk

UKERNA manages the networking programme on behalf of the higher and further education and research community in the United Kingdom. JANET, the United Kingdom's academic and research network, is funded by the Joint Information Systems Committee (JISC).

For further information please contact:

JANET Customer Service
UKERNA
Atlas Centre, Chilton, Didcot
Oxfordshire, OX11 0QS

Tel: +44 (0) 1235 822 212
Fax: +44 (0) 1235 822 397
E-mail: service@ukerna.ac.uk

Copyright:

This document is copyright The JNT Association trading as UKERNA. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from JANET Customer Service.

Trademarks:

JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

Disclaimer:

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

Availability:

Further copies of this document may be obtained from JANET Customer Service at the above address.

This document is also available electronically from: http://www.ja.net/documents/gn_ddos.pdf



© The JNT Association 2001

**Joint Information
Systems Committee**