Investigating a Denial of Service attack

GD/NOTE/001 (01/01)

> *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.*
>
> *Names and addresses have been altered. Individuals wishing to contact us for further information are invited to do so via Janet-CSIRT (irt@csirt.ja.net [1]).*

During the summer of 2000 our institution (a UK university) was identi?ed as a participant in a Distributed Denial-of-Service (DDoS) attack against a number of foreign sites. This paper brie?y summarises the technique we used to trace the machines involved - a task often complicated by the use of IP spoo?ng [1] [2] 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 ?rewall software [2] [3]. 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, traf?c 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.

Links
[1] mailto:irt@csirt.ja.net
[2] http://www.microsoft.com/technet/security/sourcead.asp
[3] http://www.zonelabs.com/