**7.2 What types of resources are targeted by such DoS attacks?**

DoS can target network bandwidth, system resources, or application resources.

**7.10 Define an amplification attack.**

In an amplification attack, the attacker spoofs the victim's address and makes requests of a server that result in more packets being received, thereby amplifying the attack.

**7.14 What defences are possible against a DNS amplification attack? Where must these be implemented? Which are unique to this form of attack?**

Preventing users from spoofing an address can prevent amplification attacks. In addition, the DNS servers can be configured so that the number of responses generated are limited.

**7.16 What do the terms slashdotted and flash crowd refer to? What is the relation between these instances of legitimate network overload and the consequences of a DoS attack?**

Slashdotted or flash crowding events are when a high number of legitimate users suddenly appear on a website, for instance if it was mentioned on some other very popular website, that can have the same effects as a DoS attack where servers are overloaded and traffic cannot get through.

**Problem 7.3 Consider a distributed variant of the attack we explore in Problem 7.1. Assume the attacker has compromised a number of broadband-connected residential PCs to use as zombie systems. Also assume each such system has an average uplink capacity of 128 kbps. What is the maximum number of 500-byte ICMP echo request (ping) packets a single zombie PC can send per second? How many such zombie systems would the attacker need to flood a target organization using a 0.5-Mbps link? A 2-Mbps link? Or a10-Mbps link? Given reports of botnets composed of many thousands of zombie systems, what can you conclude about their controller’s ability to launch DDoS attacks on multiple such organizations simultaneously? Or on a major organization with multiple, much larger network links than we have considered in these problems?**

128 kilobits/second = 16000 bytes/second

16000 bytes/second / 500 bytes/packet = **32 packets/second for each zombie**

Need 32 zombies to flood 0.5 megabyte/second link, need 125 for 2 megabyte/second link, need 625 for 10 megabyte/second link.

With a thousand bots, you could fill a 16 megabyte/second link. It would require around 100,000 bots in order to take down a gigabyte/second link. With a very massive botnet, an attacker could disable quite large targets, and perhaps multiple at a time.