78 Примеры вредоносных атак в компьютерных сетях

Cisco выделяет три типа вредоносных атак:

1. Reconnaissance Attacks -- разведывательные, целью которых является несанкционированный сбор информации.

Примеры: просмотр содержимого пакетов сниферами (packet sniffing), сканирование адресов в поисках станций (ping sweeping), сканирование портов в поисках сервисов (port scanning), ловля на доверие (phishing), социальная инженерия (social engineering), поиск информации в Internet (Internet information queries).

2. Access Attacks -- связанные с доступом, целью которых является получение несанкционированного доступа к информации или подмена информации.

Примеры: подбор паролей методом «грубой силы» (brute-force password search), использование имеющихся прав не по назначению (trust exploitation), перенаправление пользовательских запросов на ложные серверы (port redirection), различные варианты подмены информации в каналах (man-in-themiddle), использование уязвимостей ПО (buffer overflow).

3. DoS (Denial of Service) Attacks -- связанные с сервисами, целью которых является отказ в обслуживании по тому или иному протоколу.

DDos (Distributed DoS) отличается тем, атаку проводят множество станций.

Примеры: ping с длиной пакета 65535 Byte с целью «завешивания» некоторых старых ОС (ping of dead), порождение с помощью особенностей SNMP-запросов многочисленных станций-«зомби» с целью «забрасывания» SNMP-ответами выбранной станции-«жертвы» (smurf), последовательное создание многочисленных полуоткрытых TCP-соединений (TCP SYN flooding).