【CN】Day10

Created	@May 28, 2022 2:07 PM
Class	
Type	
Materials	Network Security
Reviewed	□

【Ch1】Computer Network and the Internet

1.6 Networks Under Attack

Much of the malware today is self-replicating: once it infects one host, from that host it seeks entry into other hosts over the Internet.

Viruses are malware that require some form of user interaction to infect the user's device. The classic example is an e-mail attachment containing malicious executable code.

Worms are malware that can enter a device without any explicit user interaction.

The Bad Guys Can Attack Servers and Network Infrastructure

Another broad class of security threats are known as denial-of-service(DoS) attacks.

Most Internet DoS attacks fall into one of three categories:

- Vulnerability attacks. This involves sending a few well-crafted messages to a vulnerable application or operating system. The service can stop or the host can crash
- Bandwidth flooding. The attacker sends a huge number of packets to the targeted host and prevent legitimate packets from reaching the server.
- Connection flooding. The attacker establishes a large number of half-open TCP connections at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

Let’s now discuss bandwidth flooding in more detail. If all the traffic emanates from a single source, an upstream router may be able to detect the attack and block all traffic from the source before the traffic gets near the server.

In a distributed Dos(DDoS) attack, the attacker controls multiple sources and has each source blast traffic at the target.

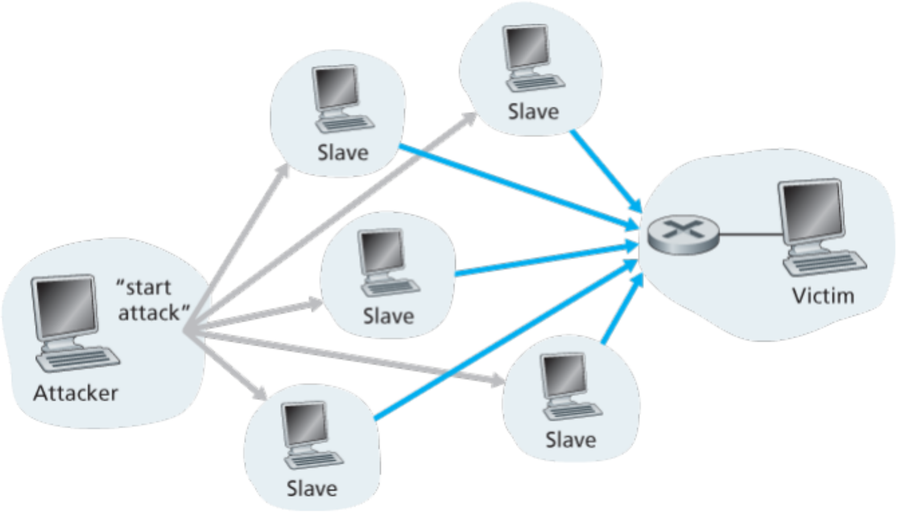

Figure 1.25 A distributed denial-of-service attack