**Smurf Attack**

**Description 1**

The attacker sends a large number of ICMP echo requests to a broadcast address. All the ICMP messages have spoofed source address as that victim’s IP address. Eventually all the reply messages target and flood the victim’s address. [1]

**Description 2**

The Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. **This can slow down the victim's computer to the point where it becomes impossible to work on. [2]**

**Description 3**

A Smurf attack is a form of a distributed denial of service (DDoS) attack that renders computer networks inoperable. The Smurf program accomplishes this by exploiting vulnerabilities of the Internet Protocol (IP) and Internet Control Message Protocols (ICMP).

The steps in a Smurf attack are as follows:

1. First, the malware creates a network packet attached to a false IP address — a technique known as "spoofing."
2. Inside the packet is an ICMP ping message, asking network nodes that receive the packet to send back a reply
3. These replies, or "echoes," are then sent back to network IP addresses again, setting up an infinite loop.

When combined with IP broadcasting — which sends the malicious packet to every IP address in a network — the Smurf attack can quickly cause a complete denial of service. [3]

**Reference**

[1] [**https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764**](https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764)

[2] <https://en.wikipedia.org/wiki/Smurf_attack>

[3] https://usa.kaspersky.com/resource-center/definitions/smurf-attack