**IP Spoofing**

**Other name: IP address forgery**

**Description 1**

IP address Spoofing occurs when the attacker determines and uses an IP address of a network, computer, or network component without being authorized to do so. **A successful attack allows the attacker to operate as if the attacker is the entity normally identified by the IP address.** [1]

**Description 2**

IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system. One technique which **a sender may use to maintain anonymity is to use a proxy server**. [2] In IP spoofing, an attacker gains unauthorized access to a computer or a network by **making it appear that a malicious message has come from a trusted machine by “spoofing” the IP address of that machine**.

**Description 3**

[3] first uses description 2 for introducing ip spoofing. What is the advantage of sending a spoofed packet? It is that the sender has some kind of malicious intention and does not want to be identified. You can use the source address in the header of an IP datagram to trace the sender's location. Most systems keep logs of Internet activity, so if attackers want to hide their identity, they need to change the source address. The host receiving the spoofed packet responds to the spoofed address, so the attacker receives no reply back from the victim host. But if the spoofed address belongs to a host on the same subnet as the attacker, then the attacker can "sniff" the reply. You can use IP spoofing for several purposes; for some scenarios an attacker might want to inspect the response from the target victim (called "nonblind spoofing"), whereas in other cases the attacker might not care (blind spoofing). ( find more about consequences in [3])

Spoofed IP packets are not always evidence of malicious intent: in performance testing of websites, hundreds or even thousands of "vusers" (virtual users) may be created, each executing a test script against the website under test, in order to simulate what will happen when the system goes "live" and a large number of users log on at once. [4]

**Description 3**

**Reference**

**[1]** [**https://technet.microsoft.com/en-us/library/dd572566(v=office.13).aspx**](https://technet.microsoft.com/en-us/library/dd572566(v=office.13).aspx)

**[2]** [**https://www.symantec.com/connect/articles/ip-spoofing-introduction**](https://www.symantec.com/connect/articles/ip-spoofing-introduction)

**[3]** [**http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-38/104-ip-spoofing.html**](http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-38/104-ip-spoofing.html)

**[4] https://en.wikipedia.org/wiki/IP\_address\_spoofing**