Detecting and Preventing IP-spoofed Distributed DoS Attacks

Thusitha Tennakoon : MS20920340

February 2021

1 Introduction

IP spoofing is the development of IP (IP) packets that have been changed to mask the sender's Identity or both to impersonate another computer device. The source IP address header field includes an address different from the current source IP address for IP spoofing. The technology of IP spoofing often employed by hackers to conduct distributed DDoS attacks and MITM attacks on targets or surrounding infrastructure. This is a strategy that is commonly used by hackers. The DDoS attack aims to conquer a traffic target while masking the malicious source's identity, preventing mitigation. Spoofed IP addresses can be used to allow attackers to: preventing authorities and forensic cyberinvestigators from being identified and involved; Prevent targeted devices from alerting unwitting and unwilling participants about attacks; Bypass authentication scripts, programs and services to mitigate DDoS attacks by blacklists of established malicious traffic sources IP addresses.

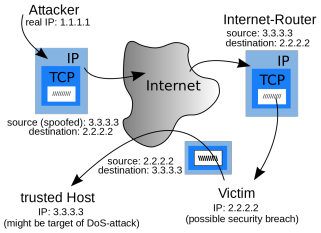

Figure 1: IP Spoofing

2 How IP spoofing works

The attacker modifies the source address in the outgoing packet header in IP Spoofing, so the destination computer considers the packet as if it comes from

a trustworthy source such as a computer in the business network and is acknowledged by the destination computer. As there are no external indicators of manipulation as the IP spoofing operation is done on the network level. In DDoS attacks, IP spoofing is widely used if hackers use spoofed IP addresses on computer servers that are largest enough to make them unusable by lawful users. IP spoofing Spoofed IP packets are often sent through geographically dispersed botnets. Huge botnets can contain tens of thousands of computers that can simultaneously spot many source IP addresses. This automatic assault is also difficult to track.

3 How to prevent IP spoofing

Organizations should take steps to prevent the infiltration of spoofed packets, including: • Atypical behavior tracking networks. • Installing packet filtering systems that are able to identify anomalies, such as outgoing packets with IP source addresses that do not conform to the network of the business. • To stop receiving spoofed packets from an intruder who has already abused a separate device on the company network using rigorous control methods for all remote access, including systems in a business intranet. • IP inbound IP packet authentication. • Use the blocker for a network attack. Firewalls are an essential tool to block spoofed-addressed IP packets, and all company routers must be designed for refusing spoofed-address packets. Such fundamental considerations are: • Setting firewalls for rejecting packets from outside the company's business perimeter with private IP addresses. • The blocking of traffic from the company inside but which spoots an external address as the source IP address, prevents the initiation of spoofing attacks within the company on other external networks.

4 Types of spoofing

Internet spoofing on various network layers can be done. In addition, spoofing in the Address Resolutions Protocol (ARP) headers takes place in the network layer (layer 3 of the OSI communications model) and in Ethernet frames bear the protocol. When an attacker sends falsified ARP messages over the local area network, an ARP spoofing attack takes place. This connects the MAC address of the hacker to the IP address of a legitimate network machine or server. Domain name system (DNS) spoofing is another form of spoofing. This form of attack exploits DNS faults and distracts internet traffic from legal servers and fake servers. By changing email header fields, hackers can spoof emails to falsely reveal that the message was sent from another sender. Spoofed e-mail typically forms part of a phishing attack that involves a link to a spoofed web site: a duplicate version of the original website. This spoofed website seeks to steal login credentials or other secrecy by tricking them to believe that they are on a legitimate site.

5 Examples of IP spoofing

On 28 February 2018, what was thought to be the largest DDoS assault ever recorded hit the GitHub hosting platform. The hackers spoofed the IP address of GitHub and transmitted queries to various servers that were normally used for accelerating database-driven sites. The servers then amplified the requested data to GitHub by a factor of about 50 so that a maximum of 51 KB is sent to the target for each byte sent by the assailant. In this case, 1.35 terabits per second of traffic was hit by GitHub and the site was reduced to 10 minutes. On 25 December 1994, hacker Mitnick Kevin attacked the rival Tsutomu Shimomura computer system using IP spoofing. In another infamous attack he launched.

universe" [2] universe" [1]

References

[1] Kaspersky. *How ip spoofing works.* Kaspersky, 2020.

[2] URL. *What is ip spoofing.* Cloud flare, 2020.