Detecting and Preventing IP-spoofed Distributed DoS Attacks

Thusitha Tennakoon : MS20920340

February 2021

1 Introduction

IP spoofing is the modification of IP (IP) packets to disguise the sender's identity or both, in order to impersonate another computer device. For IP spoofing, the source IP address header field contains a different address from the current source IP address.

IP spoofing is a technique used by hackers to launch distributed DDoS and MITM attacks on targets or surrounding infrastructure. This is a tactic that hackers frequently employ. The goal of a DDoS assault is to take down a traffic target while concealing the identity of the offending source, preventing countermeasures.

Attackers can employ spoof IP addresses to prevent authorities and forensic cyberinvestigators from being recognized and implicated; Prevent unwitting and unwilling participants from being notified of assaults by using targeted devices; Blacklists of known malicious traffic sources IP addresses are used to bypass authentication scripts, applications, and services in order to minimize DDoS attacks.

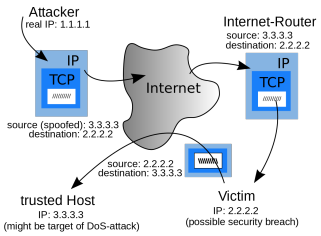

Figure 1: IP Spoofing

2 How IP spoofing works

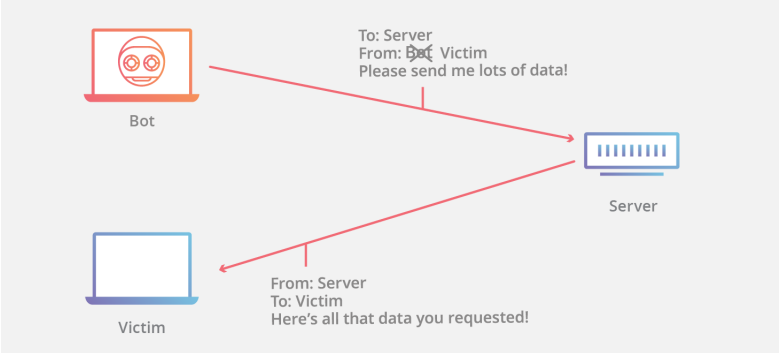

Figure 2: IP Spoofing

In IP Spoofing, the attacker alters the source address in the outgoing packet header such that the destination computer treats the packet as if it came from a reliable source, such as a computer in the business network, and accepts it. Because the IP spoofing process is performed at the network level, there are no external indicators of manipulation.

IP spoofing is extensively used in DDoS attacks where hackers utilize faked IP addresses on computer systems large enough to render them unusable by lawful users. Spoofing an IP address Botnets that are geographically scattered are frequently used to send spoof IP packets. Botnets with tens of thousands of machines can detect many source IP addresses at the same time. 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, among other measures, should be taken to avoid the penetration of faked packets. • Putting in packet filtering technologies that can spot irregularities such outgoing packets with IP source addresses that don't match the company's network.s.

• Using strict control techniques for all remote access, including systems in a business intranet, to prevent receiving faked packets from an intruder who has already misused a separate device on the company network. • IP authentication for inbound IP packets. • For a network attack, use the blocker. Spoofed-addressed IP packets must be blocked by firewalls, and all enterprise routers must be programmed to refuse spoofed-address packets. The following are some of the most important considerations: • Configuring firewalls to reject packets with private IP addresses from beyond the company's corporate boundary. • Blocking traffic from within the company that spoofs an external IP address as

the originating IP address avoids spoofing attacks on other networks within the firm.

4 Detection of Attacks

Figure 3: IP Spoofing

We utilize a counter called Total-Mismatches-Counter (TMC) to detect the beginnings of a DDoS attack.the amount of packets whose markings are impossible to match at the perimeter of the firewall Both packets with improper marks and packets from unknown sources fall into this category.addresses that haven't been entered into the Filter Table

5 Types of spoofing

It is possible to spoof the internet at many network layers. Spoofing in the Address Resolutions Protocol (ARP) headers occurs on the network layer (layer 3 of the OSI communications model) as well as in Ethernet frames that carry the

protocol. An ARP spoofing attack occurs when an attacker transmits false ARP packets over a local area network. The hacker's MAC address is linked to the IP address of a genuine network computer or server in this way. Another type of spoofing is domain name system (DNS) spoofing. This type of attack takes use of DNS errors to divert internet traffic away from legitimate and impostor servers. Hackers can spoof emails by modifying email header data to make it appear as if the message came from a different sender. Typically, faked e-mail is part of a phishing attack that includes a link to a spoofed website, which is a copy of the original website.

6 Examples of IP spoofing

On February 28, 2018, the GitHub hosting platform was targeted by what was thought to be the greatest DDoS attack ever recorded. The hackers fake GitHub's IP address and send requests to multiple services that are usually used to speed up database-driven websites. The servers then multiplied the data transmitted to GitHub by around 50, sending a maximum of 51 KB to the target for each byte sent by the attacker. In this example, GitHub received 1.35 terabits per second of traffic, and the service was down for 10 minutes. Mitnick Kevin, a hacker, used IP spoofing to attack the competitor Tsutomu Shimomura computer system on December 25, 1994. He launched yet another infamous onslaught.

7 Spoofing Attack Prevention and Mitigation methods

Organizations can use a variety of technologies and strategies to mitigate the potential of spoofing attacks. Organizations can take the following steps to prevent spoofing attacks:

Packet filtering: Packet filters examine packets as they go over a network. Packet filters are important in preventing IP address spoofing attacks because they may filter out and block packets with conflicting source addresses (packets from outside the network that show source addresses from inside the network and vice-versa)

Avoid trust relationships: Organizations should design protocols that rely as little as feasible on trust relationships. Because trust relationships only require IP addresses for authentication, it is much easier for attackers to carry out spoofing attacks when they are in place.

Use spoofing detection software: Many applications are available to assist enterprises in detecting spoofing attacks, especially ARP spoofing. These programs verify and certify data before it is transferred, and they prevent data that appears to be faked.

Use cryptographic network protocols: Secure communications protocols such as Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure

(HTTPS), and others help to prevent spoofing attacks by encrypting data before it is delivered and authenticating it as it is received.

8 Conclusion

IP spoofing will be less of an issue after everyone switches to IPv6, because IPv6 provides encryption and authentication. Until then, end users attempting to prevent MITM should be cautious when utilizing public WIFI to do critical transactions such as banking. They should also ensure that the websites they visit use the HTTPS encryption protocol.

Unfortunately, DDoS attacks are significantly more difficult to counteract. To survive these attacks, a lot of hardware equipment is necessary, thus the most cost-effective option is to sign up for a good DDoS protection service.

IP spoofing is an issue with no simple solution because it is built into the TCP/IP suite. Understanding how and why spoofing attacks are carried out, as well as a few easy preventative measures, can help protect your network against malicious cloaking and cracking techniques.

universe" [2] universe" [1]

References

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

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