Enhancing Packet Filtering via a Reverse IP/Domain Check

Posted on January 9, 2020

Spoofing is a cyber attack method where the adversary impersonates a legitimate user to gain access to a network or device. Once inside the target network, the attacker can then perform large-scale attacks, steal sensitive information, and inject systems connected to the network with malware.

Although there are several types of spoofing, the most common being IP spoofing. This method allows attackers to launch denial-of-service (DoS) and man-in-the-middle (MitM) attacks, two of today's most prevalent cyber attack types. At present, we see 30,000 DoS attacks per day, whereas MitM attacks account for 35% of exploitations that target inadvertent system or software weaknesses.

The statistics may seem overwhelming, but there are strategic processes such as packet filtering that can help organizations avoid these attacks. This post features a reverse IP domain check tool — Reverse IP/DNS API — which makes packet filtering effective across the various implementation systems or technologies an organization uses. But first, let us examine how IP spoofing is used to launch DoS and MitM attacks to understand why it is crucial to detect IP spoofing.

IP Spoofing: A Means to Launch DoS and MitM Attacks

IP spoofing takes advantage of the natural way in which the Internet works — sending packets back and forth as a way for computers and networks to communicate with one another. Attackers tweak the source address in the IP packet header to trick the receiver into thinking that the traffic's source or sender is trustworthy.

In DoS attacks, adversaries typically infect thousands of devices with malware (usually without their owners' knowledge), effectively creating a botnet under their complete control. The attackers then initiate a communication request to all the bots (infected computers, also known as "zombies"), but they replace the source IP address with that of the target first. When the bots respond to the communication, all traffic goes to the target website until it gets flooded and

consequently becomes unavailable.

MitM attacks work differently but still involve IP spoofing. The attackers listen to the communication between two computers, without their owners' knowledge, of course. They then relay and alter data packets, allowing them to obtain sensitive information.

DoS attacks can be launched as revenge, although some attackers also do them for money. In the latter case, they usually would terminate the attack when the website owner sends payment. The goal of MitM attacks, on the other hand, is to steal sensitive information such as bank details, login credentials, credit card numbers, and other personally identifiable information (PII). This data can then be sold in underground markets or used to further attack the owner.

These cyber attacks can turn out very costly for affected parties, and organizations must beef up their security infrastructure by nipping them in the bud and deal with IP spoofing before the altered IP addresses are granted network access.

Dealing with IP Spoofing through Packet Filtering

What Is Packet Filtering?

Since DoS and MitM attacks are enabled by IP spoofing, it makes sense to detect spoofed IP addresses and deny access to them. This process is what packet filtering is all about — allowing or blocking outgoing and incoming packets according to predefined rules.

Packet filtering can be performed by using security technologies such as firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), log monitoring devices, or security information and event management (SIEM) solutions.

Strengthening Packet Filtering Systems with Reverse IP/DNS API

Regardless of the system an organization uses for packet filtering, it should possess these inherent capabilities:

- Inspection of each data packet and its headers
- Predefined rules to tell the system what to do to a packet after inspection
- Execution of the actions defined by the rules

Upon inspection, the source IP address can be compared with the data returned by Reverse IP/DNS API. If the source IP address is associated with domains tagged as suspicious during the **reverse IP/domain check**, the packet should be rejected.

Consider a scenario where an attacker launches a DoS attack on a network. If the target organization uses an enhanced packet filtering system with Reverse IP/DNS API, the suspicious packets tied to the attack have better chances of being automatically rejected. The attack is then less likely to push through, and business disruptions are mitigated.

Cyber attackers do not typically discriminate when it comes to choosing targets. Small businesses and large organizations play fair, as long as they have insufficiently protected infrastructures. As such, any enterprise with an online presence needs to employ different tools to strengthen its security posture.

One such tool is Reverse IP/DNS API, which helps security teams perform **reverse IP/domain checks** to see if particular suspicious domains are hosted on the same source IP address specified in a data packet. This tool triggers an alert, allowing the user to deny spoofed packet access to its network, effectively reducing the risk of a costly cyber attack. Note that Reverse IP/DNS API is a RESTful API, which means it can be easily integrated into the aforementioned software solutions.