Medicon Engineering Themes
Volume 7 Issue 5 November 2024
Article Type: Editorial
ISSN: 2834-7218

Network Security Approach to Mitigate Risks of using Black-listed IP Addresses

Roshan Chitrakar*

Nepal College of Information Technology, Nepal

***Corresponding Author:** Roshan Chitrakar, Nepal College of Information Technology, Nepal.

Received: October 02, 2024; **Published:** November 05, 2024

Introduction

A few network security communities of security practitioners, researchers, hackers, attackers etc. frequently use Black-Listed IP addresses; they also use them as target IP addresses for exercising various network attacks while learning and practicing hacking or security analysis. These IP addresses may be in previous few occasions black-listed or blocked; if not, they may get eventually be black-listed too. A few ISPs in developing and least developing countries purchase such black-listed or blocked IP addresses (BLIP) in much cheaper price and distribute to their Internet users.

There are risks of using BLIPs as the community of white-hat and black-hat hackers, intentionally or being unknown that the IP addresses they have been using no longer belong to them, may still be using them as the target as usual. Thus, the Internet clients using BLIPs (assigned by their ISPs) may be victimized of various attacks without knowing that their computers and network devices have been assigned with bad IP addresses. There are professional and legal issues too in addition to the issue of business ethics and they must be addressed in a proper manner. Here, in this editorial, I am proposing network security approaches to mitigate risks occurring in using such addresses. The ISPs can implement these approaches while the issues are being resolved.

The Approach

It is not always necessary that the devices, even after using BLIPs, are attacked or compromised; they may be safe most of the time. So, I suggest designing, developing and deploying an Intrusion Detection System (IDS) that warns as soon as an intrusion or attack occurs. The IDS model can be built by making it learn in various security scenarios. In the following sections, I am explaining the scenarios of using BLIPs and ways to design the IDS.

Scenario #1

A web environment is setup by configuring BLIPs to Web servers and put them in De-Militarized Zone (DMZ) to allow maximum possible attacks. User authentication logs are collected. A clustering method is applied to make several smaller clusters from the large data of logs collected so that a classification technique can be applied in parallel fashion. Thus, an IDS model is learnt, trained and built.

Scenario #2

The configuration is made like the scenario #1 but the web servers are placed inside a Firewall or a security control. User authentication logs are collected; clustering and classification are performed. Thus, the IDS model is further learnt, trained and built.

Scenario #3

The configuration of the scenario #1 is copied and SSL certificates are installed in the web servers. The experiment is repeated, and the IDS model is updated again.

Scenario #4

The configuration of the scenario #2 is copied and SSL certificates installed, experiments repeated, and the IDS model finally updated.

Conclusion

It is no doubt that use of BLIPs must be discouraged but it may economically help the less and least developing countries. So, technological trade-offs may be applied; and the proposed approach serves the purpose. It also makes the re-use of BLIPs possible, instead of dumping them permanently. However, IDS model alone is not enough to protect completely from vulnerabilities due to BLIPs and hence the ways of prevention mechanism should also be integrated with the proposed IDS model.

Volume 7 Issue 5 November 2024