Testing Resilience of Router against Denial of Service Attacks

Vishal Maruti Karande[1], Sandeep Nair Narayanan[1], Alwyn Roshan Pais[1], and N. Balakrishnan[2]

[1] Information Security Lab, Dept. of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, India - 575025
{vishalmkarande,sandeepnairnarayanan,alwyn.pais}@gmail.com
[2] Dept. of SERC, Indian Institute of Science, Bangalore, India - 560012
balki@serc.iisc.ernet.in

Abstract. Provisioning data security and integrity in an IP network requires a detailed understanding of both the architecture and the performance of devices that are used within the network. A router interconnects two or more computer networks, and it becomes most common target for attackers to carry out Denial of Service Attacks. Thus it is necessary to study the effect of resource exhaustion attack on router with respect to its performance and security. In this paper, the proposed framework provides an effective method to evaluate router performance and its resilience against denial of service attacks. The feasibility of the framework has been demonstrated by carrying out different resource exhaustion attacks on device under test (DUT) i.e. router, and the resilience against the attacks is measured using a defined set of performance metrics.

Keywords: Denial of service attacks, Performance Testing, Resilience, Router Performance.

1 Introduction

Today most organizations are dependent on the performance and security of their network infrastructures. Building and securing network infrastructure in both normal and attack scenarios require a detailed understanding of the performance of devices that constitute the network infrastructure [12]. Enterprise networks are commonly based on a three tier model. The first layer includes Access Routers located in small offices which do not require hierarchical routing of their own. The second layer includes Distribution Routers which aggregate data from multiple Access Routers. These routers provide functionalities like QoS, VPN etc. The third layer includes the Core Routers which form the backbone network interconnecting different Distribution Routers. As router interconnects two or more computer networks by providing packet routing service, it becomes the most common target for attackers to carry out denial of service attacks.

Today different varieties of routers are provided by router vendors like Cisco, Juniper, Linksys etc. each having its own resilience against security attacks.

D.C. Wyld et al. (Eds.): NeCoM/WeST/WiMoN 2011, CCIS 197, pp. 107–116, 2011.

Resilience is the ability of the router to cope with stress and adversity. Active routers offer the combined benefits of intrusion detection, firewall protection and work collaboratively to provide resilience against security threats. However combining all security measures in a single device for defense against security threats can result in a significant performance loss. Thus router vendors have to find balance point between performance and security while providing functionalities like QoS, VPN etc. Efficient router testing for finding its resilience level helps in building performance and security balance point.

This paper focuses on the generic router resilience testing framework independent of router architecture and underlying protocols, analyzing the potential threats and entry points. We have performed various denial of service attacks on device under test (DUT) i.e. router and performance of the router is measured with respect to performance metrics such as throughput (connections per second, packets per second), scalability, request/response delay, transaction duration, allocation of resources etc.

2 Background

2.1 Traffic Types

The different types of traffic handled by the routers include Transit IP packets, Receive IP packets and Exception IP/Non-IP Packets as shown in Fig 1.

- *Transit IP Packets.* These are the packets with the destination IP address which is not owned by any of the interfaces of the router, but an IP address which is accessible through the router. When a router sees a transit packet, the decision it makes is to forward the packet out to one of its interfaces.
- *Receive IP Packets.* IP packets that arrive at a router, and that are destined to an IP address owned by that router itself are called receive-adjacency packets. With receive-adjacency packets, the router cannot engage any specialized forwarding hardware; the router must process the packet itself using its own local CPU resources.

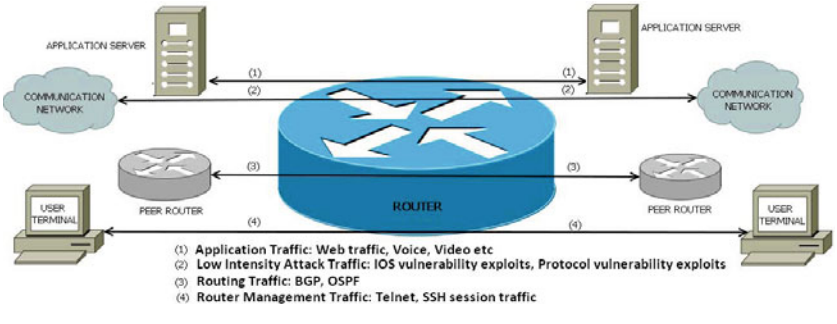

Fig. 1. Router Traffic