

Introduction

In this fast-moving Internet-driven world, the attacks are changing rapidly. The list of attacks is huge and the networks attacked are global in nature. All attacks are not possible to be tried out in real networks because of resource limitation or security concerns. Hence, the need for a Network Security Simulator (NSS)* is essential.

We have successfully built a framework for simulating network security using existing Network Simulator NCTUns (National Chio Tung University network simulator). The Simulator is UNIX/Linux-based platform.

NSS Architecture

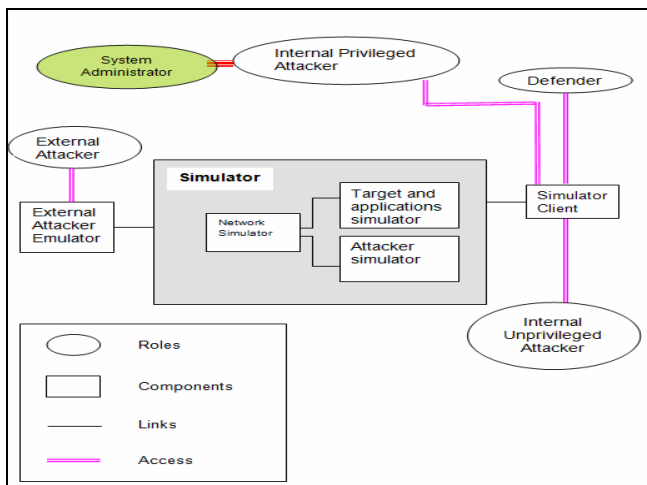


Figure 1 NSS Architecture

The Integrated Network Security Simulator system architecture is shown in Figure 1. The integrated security simulator consists of the Network Simulator, the Security attacking tools, Target and other applications, and the Simulator client. The simulator is the core component of the system and it further comprises the Network Simulator, Attacker Simulator, and the Applications Simulator.

Example: SYN flood attack Simulation with NSS

The SYN attack exploits TCP/IP three-way handshake. In a normal three-way handshake, the client sends a SYN packet to the host, the host replies to this packet with a SYN ACK acknowledgement packet. Then the client responds with a TCP ACK packet.

The complete simulated network, shown in Figure 2, consists of 3 routers, 4 switches, and 18 workstations. The attackers are Nodes 12 and 15, Web server Node 22 (Target), Legitimate User Node 3, Router R1 Node 19, and Firewall Router R2 Node 18. The bandwidth of each link is set to 10 Mbps.

Initially the legitimate user is downloading data at 1200 KBps from the Web server. But as soon the attackers execute the

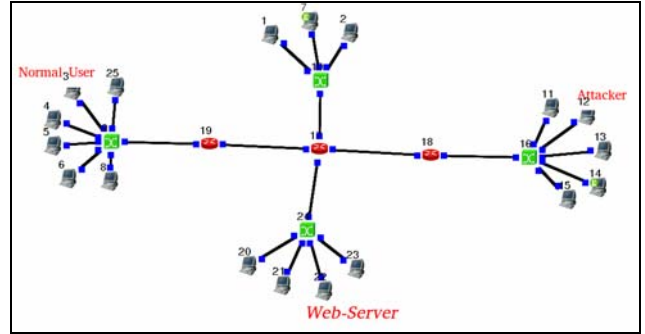


Figure 2 Network Topology for SYN attack

SYN attack, the connection table of the Web server is filled up and the file transfer rate goes down to about 20 KBps. Figure 3(a) shows a sudden increase in traffic at the Web server due to SYN packets starting at 40 seconds, and reaches a maximum at 42 seconds. Figure 4 shows the very low downloading rate of about 20 KBps between download rate of 7,000 and 12,000 KBps during SYN flood attack. The duration of SYN attack effect on file transfer is longer (about 2 to 3 minutes) than SYN attack duration (8 seconds) because the Web server has queued up half open TCP connections caused by SYN attack waiting for response from client. After the half open TCP connections close by timeouts, which by default is 75 sec, file transfer rate recovers to normal. The SYN flood attacks in the example are stopped activating the firewall in R2 at 46 seconds. The SYN packets are cleared at 48 seconds and normal service is restored, Figure 3 (b).

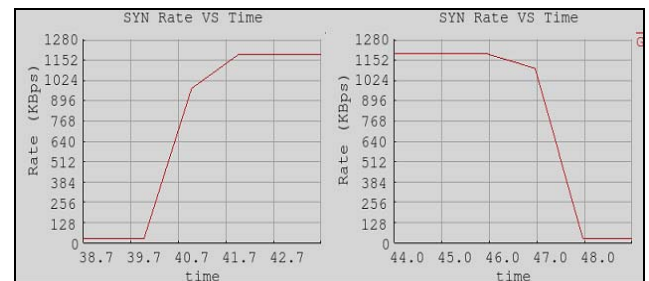


Figure 3(a) Traffic at Web Server during SYN attack
(b) after Firewall activation

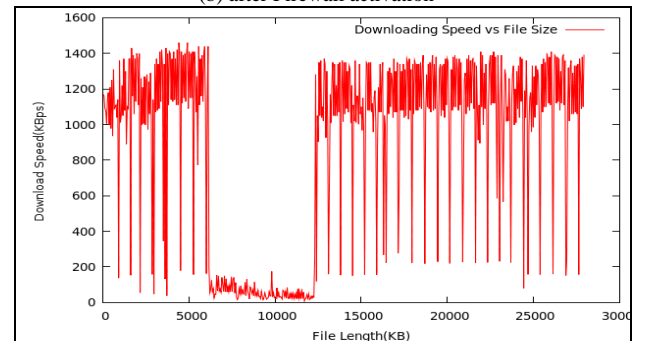


Figure 4 Downloading Speed vs. File Size

A. Singh did a B.Tech project on simulators, and D. Tripathi on security attacks in 2008