Linux Firewall Overview

Disclaimer: This assignment is based on Linux Firewall Exploration Lab, Copyright © 2006 - 2013 Wenliang Du, Syracuse University, All rights reserved.

The learning objective of this lab is for students to gain insights into how firewalls work by playing with firewall software and implementing a simplified packet filtering firewall. Firewalls have several types, and the two most commonly known are the packet filter and application-level gateway (application firewall). Packet filters act by inspecting the packets; if a packet matches the packet filter's set of rules, the packet filter will either drop the packet or forward it, depending on what the rules say. Packet filters are usually stateless; they filter each packet based only on the information in that packet, without paying attention to whether a packet is part of an existing stream of traffic. Packet filters often use a combination of the packet's source and destination addresses, protocol, and port numbers for TCP and UDP traffic. In this assignment, the focus is on packet filtering firewalls.

Organization

This assignment is done individually.

Requirements and points

For this assignment, you can get a maximum of 100 points. There are two tasks; Task 1 is mandatory, and Task 2 is optional. **To pass this assignment, you must complete Task 1 Quiz with at least 35 points and Task 1 Submission with at least 15 points.** If you fail Task 1, you will automatically fail this assignment and get 0 points for Task 2 (i.e., your points in Task 2 are discarded).

The grading scale is as follows:

- Task 1: 60 points
  - Quiz: 40 points
  - Submission: 20 points
- Task 2: 40 points
  - Quiz: 15 points
  - Submission: 25 points

Note that there can be a deduction in points depending on the quality of the submissions. For instance, if you aim for 100 points, but we assess that your submission only solves half of the challenges in a satisfactory manner, you might get 80 points.

If you fail the assignment, you have a second chance to complete the assignment in the endgame. However, the grading scale gives 75% of the original number of points. Consequently, you must do both task1 and task2 to pass the assignment.

To pass the endgame, you must fulfill two criteria below:

- Complete Task 1 Quiz with at least 35 points and Task 1 Submission with at least 15 points before the 75% grading scale is applied
- Score at least 50 points after the 75% grading scale is applied

Supervision and guidance

We use the discussion forum as the main communication channel. Therefore, make sure you subscribe to it! If you have questions, get stuck, or have experiences or tips that you want to share with other students, please feel free to use this discussion topic. The teaching staff monitors this discussion topic, but we also encourage students to help and discuss with each other.

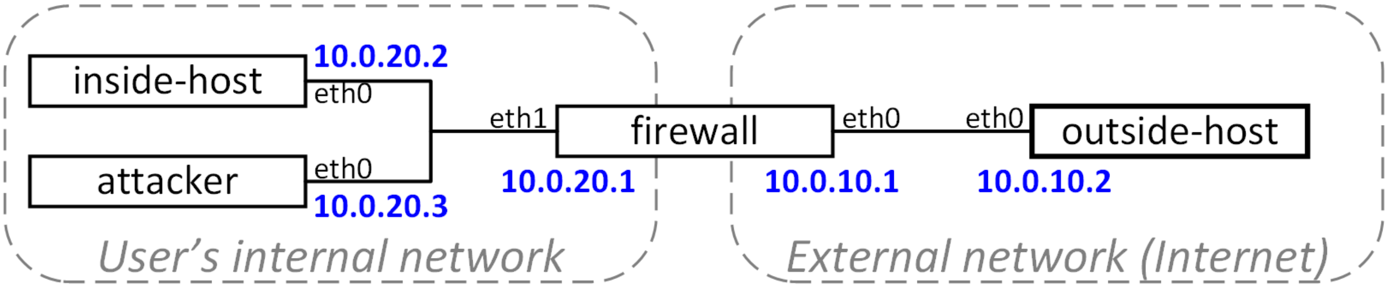
Lab environment

This lab should be performed on the lab VM. More details can be found on **instructions for setting up the course virtual machine (https://canvas.kth.se/courses/31174/pages/instructions-for-setting-up-the-course-virtual-machine-vm-without-ga)** .

Network setup

You will conduct this lab using a network topology shown in the figure below with four machines: a firewall, an inside host, an outside host, and an attacker. These machines have already been set up using LXC containers inside the lab VM. The network topology contains two subnetworks: the external network: 10.0.10.0/24, and the internal network: 10.0.20.0/24. The external network represents the Internet. The internal network represents the user's internal network. The firewall serves as the gateway that interconnects the internal and external networks. In this assignment, we assume that the attacker is a compromised host inside the user's network.

Topology



Tools

- wireshark - Sniffer and protocol analyzer
- tcpdump - Command-line based sniffer
- netwox - Tools to generate packets and spoof network traffic

- netcat (nc) - A tool for reading/writing network connections using TCP/UDP, which can be used for a simple client/server.
- iptables - tool to configure the tables provided by the Linux kernel firewall (Netfilter modules)
- ufw - a firewall configuration tool for iptables (ufw = uncomplicated firewall)