Politecnico di Milano

Progetto di Piattaforme Software per la Rete - Modulo 2

Port Knocking

Authors:
Andrea Mariani
Jacopo Fiorenza
Filippo Garolla

Supervisor:
Dr. Alessandro Barenghi

June 18, 2013

Contents

1 Introduction

In computer networking, port knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of pre-specified closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific port.

2 Module Functionality

Once this module is loaded into the kernel, it is called every time a packet reaches a network interface.

It listens to every TCP SYN packet, looks for the correct sequence and meanwhile it drops every TCP packet coming at the blocked ports. When the sequence is matched, a new rule is added to the firewall, using Netfilter, allowing the remote host to connect. The host can communicate on the opened port for a certain period of time, then the port is closed.

3 How To Use

Usage is very simple. You can choose to use this module setting your own sequence, port and timeout or just use the default settings.

3.1 Loading module without parameters

You can load the module without parameters, thus using the default parameters.
The default parameters are:

- port sequence: 80, 81, 82, 83, 84, 85, 86, 87
- controlled port: 10090
- timer: 20 seconds

3.2 Loading module with parameters

If you want to use your own settings you just need to load the module with the following parameters:

- port_seq=<port knocking sequence>
- port_dest=<port to open on match>
- rule_timer=<time you want to keep the port open[milliseconds]>

Ex. insmod port.ko port_seq=80,81,82,83,84,85,86,87 port_dest=10090 rule_timer=20000

You can choose to use all parameters or just the ones you need.
You can set a sequence comprising 2 to 10 ports. If you try to insert a longer sequence it will be automatically set to default.
Unspecified or incorrect parameters will use the default settings.