Workshop in Information Security – Assignment 4

Lior Peleg-Lieblich

In this assignment I added to the stateless firewall an ability to statefully track TCP connections, and accept packets from an accepted connection which conform to the current connection state. This was done in the function `conn_filter` of the new file `conns.c`, to which the firewall sent the relevant packages.

Afterwards, I added proxying abilities which allow to filter according to the actual data/payload. This was done by rewriting the IP/TCP headers in the appropriate places. Of course, I also made sure that the proxy does not "confuse" the connection tracking.

Then, I created user-space programs that forwarded the packets, and performed the required filtering (described below). In the client-to-server case, I sent to the kernel the new port used by the forwarding connection, using a dedicated sysfs driver. That allowed the kernel proxy to identify the right connection in the server-to-client traffic (note that I rewrote the port in the kernel hook).

The actual user-space filters were actually simple. The HTTP filter simply examined the response header and looked for the disallowed content types. The FTP "filter" looked for the advertisement of a data connection port and send it to the kernel through a driver, which enabled the kernel to allow incoming active FTP connections (usually only the client can initiate TCP connections).