Amplification Attack Detection using Active Measurements

Amplification attacks are a special type of DDoS attacks, where the response packet is significantly larger than the request packet. Research has shown that amplification attacks in protocols are widespread. In this thesis you will build a framework which is able to leverage active measurements to detect services which can be abused as amplifiers. The framework incorporates ZMap and its IPv6 counterpart to scan for abusable services on different UDP ports. You will implement the framework as an extensible architecture, so that future protocols can be added easily. Finally, the software will be evaluated by running periodic active measurements within a large university network. In addition, a notification module can alert affected parties.

---

Motivation

Interested, motivated, autonomous work ethic

Experienced in programming and data analysis

You live the GIYF motto

---

Requirements

Oliver Gasser  gasser@net.in.tum.de
Simon Bauer  bauersi@net.in.tum.de
Stefan Metzger  stefan.metzger@lrz.de

http://go.tum.de/306574