Technische Universität München
Lehrstuhl für
Netzarchitekturen & Netzdienste
Prof. Dr. Georg Carle

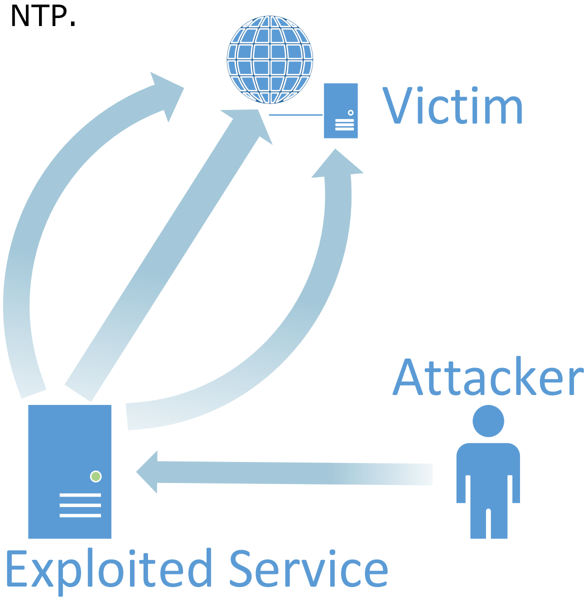
Thesis (MA/BA/IDP)

Real-time Amplification Attack Detection

Motivation

Amplification attacks are getting more common in today’s Internet. They are mostly used as part of (Distributed) Denial of Service attacks (DDoS). There have been examples of amplification attacks which used DNS. They have, however, also been used in combination with other protocols such as the network management protocol SNMP or the time protocol NTP.

Amplification attacks involve three parties: (1) The attacker, (2) the exploited service, and (3) the victim. The attacker sends requests to an exploited service. The exploited service which acts as a kind of proxy, subsequently sends response packets to the victim. These packets, however, are much larger than the request packets. The generated bandwidth for DDoS’ing the victim is thus amplified. In addition to exhausting the service capability of the victim an amplification attack produces a massive amount of traffic in the network of the exploited service.



In a previous Master Thesis we created a framework to detect Amplification Attacks. The system uses flow data as well as packet data as input. It then tries to distinguish ‘normal’ traffic from amplification attacks according to specific characteristics. The framework, however, is not yet fully automated and needs manual intervention to detect and react to attacks. Additionally, the detection parameters need a bit more tweaking and further real-world runs should be performed.

Your Task

Your task is to build upon the already existing Amplification Attack toolchain. Extend the tools to make them as automated as possible. Add configuration options to configure the reaction to detected attacks (e.g. sending email to admin). Create a web GUI to visualize the current attacks and evaluate your findings. Good programming skills and knowledge about computer networks are required.

Contact

Oliver Gasser <gasser@net.in.tum.de> Tel.: 289-18005

Felix von Eye <Felix.VonEye@lrz.de> Tel.: 35831-8876