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

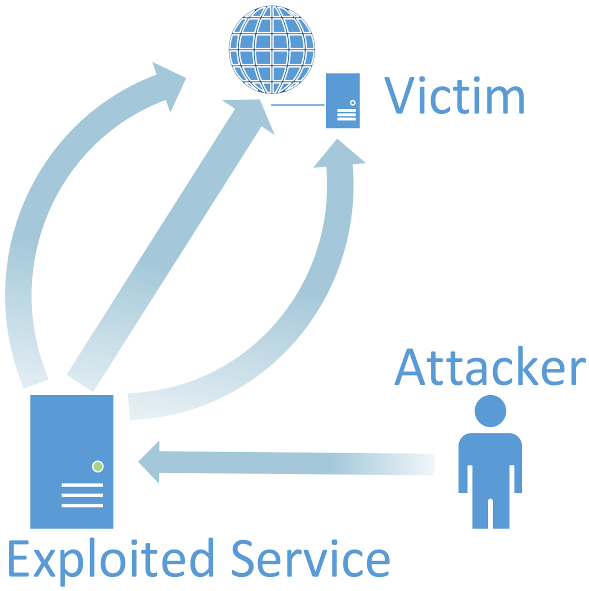
Thesis
(MA/BA/IDP)

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.

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.



Amplification attacks are generally possible with all kinds of protocols that are based on UDP. The connectionless nature of the transport protocol allows to use a fake source IP address. The attacker claims that the requests are coming from another host which will then be overwhelmed by the responses. Another prerequisite to stage an amplification attack is that the exploited service allows connections with (faked) source addresses associated with the victim. A variation are reflection attacks. They don’t amplify the traffic volume, however, still redirect traffic directed at the exploited service to the victim.

Your Task

Your task is to evaluate currently known amplification and reflection attacks. Find patterns and ways on how to recognize them in gateways to large networks. Identify common properties of these kinds of attacks and generate rules for detecting them. Additionally, evaluate other protocols for their vulnerability potential regarding amplification attacks.

Contact

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

Lothar Braun <braun@net.in.tum.de> Tel.: 289-18010