Distributed Denial of Service Attacks

Magnus Krane

magnkr@stud.ntnu.no
TTM4135 Information Security
March 22, 2013

Abstract

This paper is a lab report from the "Web Security Lab" which is a term assignment in the course TTM4135 at NTNU.

1 Introduction

2 Discussion

Denial of Service (DoS)

A denial of service attack prevents or inhibits the normal use or management of communications facilities [1]. A attacker have many ways to make the service unavailable for legitimate users. This can be manipulating networks packets, programming, or resources handling vulnerabilities among others [3]. Flooding of a network with information is the most common and obvious type of DoS attack. This could be such as loading a web page.

When you type a URL for a website into your browser, the browser sends a request to the server hosting the website. The server can only handle a certain amount of request at once. This means that if the attacker is the flooding the network with request, the server can't process your request [4].

Distributed Denial of Service (DDoS)

3 Conclusions

References

[1] William Stallings, *Cryptography and Network Security - Principle and Practice.* Fifth edition, Prentice Hall, 2011.

[2] Ross Anderson *Security Engineering. Second edition*, Wiley Publishing, 2008.

[3] Owasp.org *OWASP, Denial of Service.*
https://www.owasp.org/index.php/Denial_of_Service

[4] U.S. Department of Homeland Security *US-CERT, Understanding Denial-of-Service Attacks.*
https://www.us-cert.gov/ncas/tips/ST04-015