EFFECTS OF DENIAL OF SERVICE ATTACK AND TRAFFIC SHAPING ON SERVER SURVIVABILITY

CHINAWAT WONGVIVITKUL

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2006

ISBN 974-04-7278-8

ผลกระทบของการโจมตีแบบ Denial of Service และการบีบจราจรเครือข่ายต่อความอยู่รอดของเครื่องแม่ข่าย (EFFECTS OF DENIAL OF SERVICE ATTACK AND TRAFFIC SHAPING ON SERVER SURVIVABILITY)

ชินวัฒน์ ว่องวิวิธกุล 4437400 SCCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการควบคุมวิทยานิพนธ์: สุดสงวน งามสุริยโรจน์, Ph.D., วัสกา วิสุทธิวิเศษ , Ph.D.

บทคัดย่อ

ปัจจุบันระบบ Internet มักถูกโจมตีอย่างต่อเนื่องจากผู้บุกรุกด้วยวิธีต่างๆและเป็นสาเหตุทำให้เกิดความเสียหายอยู่บ่อยครั้ง การโจมตีเครือข่าย Network ที่เกิดขึ้นเป็นประจำและมีการศึกษากันอย่างกว้างขวาง คือ การโจมตีแบบ Denial of Service (DoS) และ Distributed Denial of Service (DDoS) ซึ่งในระบบตรวจจับผู้บุกรุก (Intrusion Detection System) ที่ได้รับความนิยมคือ Snort [9] ซึ่งเป็น Open-source ซอฟต์แวร์ Snort ดำเนินการตรวจจับผู้บุกรุกได้ทั้งแบบ Signature และ Anomaly Detection แต่ว่าไม่สามารถแยกรูปแบบที่ผิดปกติใน traffic ที่โจมตีเข้ามาได้ ดังนั้นบาง traffic ที่ต้องสงสัยอาจจะมีผ่านเข้าไปยัง server ปลายทางได้

พวกเราได้ทำการแยก Network traffic ออกเป็น 3 ประเภท คือ normal, suspicious และ malicious. Normal Traffic จะปล่อยให้ผ่านไปยังเครื่องแม่ข่ายปลายทางได้ตามปกติ แต่เราได้นำเทคนิคของการบีบ traffic (traffic shaping) มาใช้กับการจราจรแบบ Suspicious และ Malicious เพื่อทำการกำหนด bandwidth ของ traffic ที่โจมตีก่อนที่ traffic เหล่านั้น จะไปถึงเครื่องแม่ข่ายปลายทาง ในงานวิจัยพวกเราเสนอ model ที่วัดค่าความอยู่รอดของ Web Server ภายใต้การโจมตีแบบ DoS และ DDoS และใช้วิธีการป้องกันโดยใช้ Filtering rule. ค่าความอยู่รอดของเครื่องแม่ข่ายจะถูกวัดโดยใช้ timeout เป็นตัววัดว่าเครื่องแม่ข่ายที่ให้บริการอยู่รอดนานเท่าไร ภายใต้การโจมตีจากผู้บุกรุก. Model ที่นำเสนอได้ทำการปรับปรุง Snort in-line โดยนำวิธีการป้องกันของพวกเราเข้าไปไว้ในโปรแกรม ผลการทดลองแสดงให้เห็นว่าระดับค่าความอยู่รอดของเครื่องแม่ข่าย ภายใต้ model ที่พวกเรานำเสนอจะสูงกว่าการใช้ snort ต้นแบบ

119 หน้า. ISBN 974-04-7278-8

EFFECTS OF DENIAL OF SERVICE ATTACK AND TRAFFIC SHAPING ON SERVER SURVIVABILITY

CHINAWAT WONGVIVITKUL 4437400 SCCS/M

M.Sc.(COMPUTER SCIENCE)

THESIS ADVISORS: SUDSANGUAN NGAMSURIYAROJ, Ph.D., VASAKA VISOOTTIVISETH, Ph.D.

ABSTRACT

Nowadays the internet has been incessantly attacked in plenty of ways, and has caused lots of damages. Network attacks frequently happen and extensively studied are so-called denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. One of the most popular intrusion detection system (IDS) is Snort [9] which is open source software. Snort performs both signature and anomaly detection, and also provides a prevention mechanism such as dropping malicious packets. However, it cannot identify anomaly patterns in attack traffic. Therefore, some suspicious traffic may have gone thru to the target server.

We categorize network traffic into three categories: normal, suspicious and malicious. Normal traffic is allowed to pass to the target server as usual, but the technique of traffic shaping is applied for suspicious and malicious traffic in order to limit the bandwidth of attacking traffic before they reach the target server. In this thesis, we propose a model that measures the survivability of a web server under DoS and DDoS attacks, and performs the prevention mechanism using filtering rules. The server survivability is measured using a timeout indicating how long the server survived under the attack. The model modifies Snort in-line by incorporating our prevention mechanism. The experimental results show that the server has a higher degree of survivability under our proposed model than the original Snort.

KEY WORDS: INTRUSION DETECTION AND PREVENTION / DOS ATTACK / TRAFFIC SHAPING / SERVER SURVIVABILITY

119 P. ISBN 974-04-7278-8