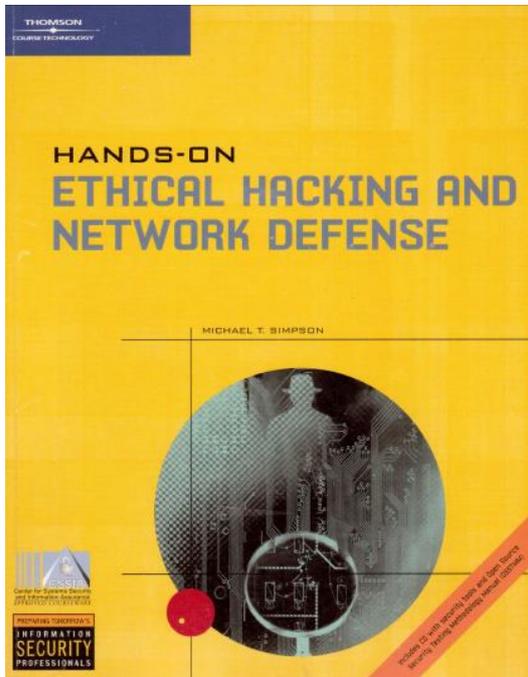


## บทวิจารณ์หนังสือ

ชัชพงศ์ อธิปัญญาวงศ์  
บริษัท อีซี บาย จำกัด (มหาชน)

doi: XXXXX



**Title:** Hands-on Ethical Hacking and Network Defense

**Author:** Michael T. Simpson

**Edition:** 2006

**Publisher:** Thomson Course Technology

**Number of pages:** 464

หนังสือ Hands-on Ethical Hacking and Network Defense เป็นหนังสือที่กล่าวถึงวิธีการและเครื่องมือสำหรับการ Hack ระบบสารสนเทศโดยเน้นที่ระบบเครือข่ายคอมพิวเตอร์เป็นหลัก และจะเน้นที่การ Hack ระบบสารสนเทศโดยเจ้าหน้าที่ของกิจการซึ่งมีเป้าหมายเพื่อสอบทานว่าระบบสารสนเทศขององค์กรมีจุดอ่อนที่ส่วนใด เพื่อจะได้จัดการติดตั้งการควบคุมต่อไป

หนังสือเล่มนี้จะแบ่งเนื้อหาเป็นบทๆ โดยกล่าวถึงภาพรวมของการ Hack ระบบสารสนเทศโดยเจ้าหน้าที่ของกิจการ ความรู้เบื้องต้นเกี่ยวกับ TCP/IP และการโจมตีระบบเครือข่าย เช่น ไวรัส DoS และ Keyloggers เป็นต้น ส่วนบทอื่นๆ จะเกี่ยวข้องกับวิธีการและเครื่องมือที่ใช้ในการ Hack ระบบสารสนเทศ โดยสรุปดังนี้

- (1) การทำ footprinting ซึ่งเป็นการเก็บรวบรวมข้อมูลขององค์กร เช่น โปรแกรมประยุกต์และที่ตั้งของระบบสารสนเทศ เป็นต้น
- (2) การ scanning ซึ่งอาจทำโดยใช้โปรแกรม เช่น Nessus เป็นต้น เพื่อค้นหาช่องโหว่ และช่องทางเข้าออกเพื่อเข้าไปทำอันตรายระบบสารสนเทศได้
- (3) การทำ enumeration เป็นการสำรวจผู้ใช้ ชื่อเครื่อง ทรัพยากรในระบบเครือข่ายและบริการต่างๆ ที่ระบบเปิดให้บริการซึ่งผู้โจมตีสามารถใช้บริการที่เปิดอยู่นั้นทำอันตรายระบบสารสนเทศขององค์กรได้
- (4) การค้นหาข้อผิดพลาดหรือการสอบทานการควบคุมต่างๆ
- (5) การเข้าถึงเป้าหมาย เช่น ขโมยข้อมูลด้วยวิธีต่างๆ เป็นต้น นอกจากนี้ยังรวมถึงการปรับปรุงข้อมูลของผู้ใช้เพื่อให้ได้รับสิทธิมากขึ้นและการซ่อนข้อมูลต่างๆ เพื่อให้สามารถกลับเข้ามาในระบบในครั้งต่อไปได้อีก