**BIS691 Internet Security (Hands-on Approach)**

**ความปลอดภัยอินเทอร์เน็ต (เชิงปฏิบัติ)**

**จำนวน 3 หน่วยกิต**

**เรียน วันอาทิตย์ 12.00 -15.00 น.**

**สอบ วันอาทิตย์ 12.00 – 14.30 หรือตามความเห็นชอบกรรมการหลักสูตร**

**วิชาบังคับก่อน (Prerequisite) :** INT606 Networking หรือ BIS606 Digital Infrastructure and Cyber Security

**สอนโดย : ดร.ตุลย์ ไตรยสรรค์**

**จำนวนที่รับ 25 คน (เรียนร่วมกัน ระหว่างนศ. IT DBIS)**

## Course description:

This course provides a comprehensive introduction to the principles and practices of internet security. Students will explore fundamental network security concepts and learn how to secure network communications by understanding the lifecycle of packets, protocol layers, and common vulnerabilities. Hands-on activities include packet sniffing and spoofing using tools such as Wireshark, tcpdump, and Scapy. Topics cover attacks on various network layers, including MAC layer attacks (ARP Cache Poisoning, Man-in-the-Middle), IP layer attacks (IP Fragmentation, ICMP attacks), and TCP protocol attacks (SYN Flooding, TCP Session Hijacking). Additionally, students will gain practical experience with firewalls (Netfilter, iptables), VPN technologies (TLS/SSL, TUN/TAP), and DNS security, addressing vulnerabilities like DNS cache poisoning and denial-of-service attacks. By the end of the course, students will have the skills to analyze, detect, and mitigate internet security threats.

**คำอธิบายรายวิชา:**

วิชานี้จะให้ความรู้เบื้องต้นเกี่ยวกับหลักการและการปฏิบัติด้านความปลอดภัยอินเทอร์เน็ตอย่างครอบคลุม นักศึกษาจะได้เรียนรู้แนวคิดพื้นฐานด้านความปลอดภัยของเครือข่าย และวิธีการป้องกันการสื่อสารในเครือข่าย ผ่านการเข้าใจวงจรชีวิตของแพ็กเก็ต ระดับชั้นของโปรโตคอล และช่องโหว่ทั่วไป กิจกรรมภาคปฏิบัติประกอบด้วย การดักจับและปลอมแปลงแพ็กเก็ต โดยใช้เครื่องมือต่างๆ เช่น Wireshark, tcpdump และ Scapy หัวข้อที่ครอบคลุมได้แก่ การโจมตีในเลเยอร์ MAC (การปลอมแปลงแคช ARP, การโจมตีแบบ Man-in-the-Middle), การโจมตีในเลเยอร์ IP (การแบ่งแพ็กเก็ต IP, การโจมตีด้วย ICMP) และการโจมตีโปรโตคอล TCP (การโจมตีแบบ SYN Flooding, การแย่งชิงเซสชั่น TCP) นอกจากนี้ นักศึกษาจะได้เรียนรู้การใช้งานไฟร์วอลล์ (Netfilter, iptables), เทคโนโลยี VPN (TLS/SSL, TUN/TAP) และความปลอดภัยของ DNS โดยเน้นถึงช่องโหว่ เช่น การโจมตี DNS Cache Poisoning และการปฏิเสธการให้บริการ (DoS) เมื่อจบวิชา นักศึกษาจะมีทักษะในการวิเคราะห์ ตรวจจับ และป้องกันภัยคุกคามด้านความปลอดภัยเครือข่าย