TEC005: Penetration Testing

Overview:
As organizations scramble to protect themselves and their customers against privacy or security breaches, the ability to conduct penetration testing is an emerging skill set that is becoming ever more valuable to the organizations seeking protection, and ever more lucrative for those who possess these skills. In this course, you will be introduced to general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.

Prerequisites:
To ensure your success in this course, you should have:
• Intermediate knowledge of information security concepts, including but not limited to identity and access management (IAM), cryptographic concepts and implementations, computer networking concepts and implementations, and common security technologies.
• Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments**.**

COURSE OUTLINE:
DAY 1 – INFORMATION GATHERING
  • The mindset of a penetration tester.
  • Types of penetration tests.
  • Limitations of penetration testing.
  • How to create a testing infrastructure.
  • Defining rules of engagement and scoping a project.
  • Reporting
  • A pen tester's tool chest of information gathering resources.
  • Types of scans - Network sweeps, network tracing, port scans, OS fingerprinting, version scans, and vulnerability scans.
  • Network mapping.
  • Port scanning
  • OS Fingerprinting.
  • Vulnerability Scanning.

DAY 2 – GAINING ACCESS
  • Exploit categories - server-side, client-side, and local privilege escalation
  • Metasploit Framework
  • The Metepreter
  • Exploit without Metasploit
  • Backdooring
  • Transferring file techniques
  • Windows commandline for penetration tester
  • Password attack
  • Password Guessing with Hydra
  • Knowing password format in Windows and Linux
  • Dumping Windows Hash
  • Offline password attack with John the Ripper
  • Cain
  • Rainbow table attacks using Ophcrack
  • Pass-the-hash
  • attacks

DAY 3 – WIRELESS ATTACK
- Wireless Concepts
- Wireless Encryption Algorithms
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Wireless Security Tools and Penetration Testing

DAY 4 – WEB APPLICATION ATTACK
- Web application scanning and exploitation tools
- Web application manipulation tools
- Injection attacks
- Building a wireless pentest platform
- Identifying unsecured access points and peer-to-peer systems
- Identifying wireless misconfigurations
- Exploiting various wireless protocols

DAY 5 - MOBILE ATTACK
- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Security Management Guidelines and Tools
- Mobile Pen Testing

วิทยากร: อ.เอกฤทธิ์ ธรรมสถิต

- MASTER OF BUSINESS ADMINISTRATION (EXECUTIVE) DEGREE SASIN GRADUATE INSTITUTE OF BUSINESS ADMINISTRATION OF CHULALONGKORN UNIVERSITY
- MASTER OF SCIENCE, MAJOR IN INFORMATION Technology Faculty of Information Technology KING'S MONGKUT INSTITUTE OF TECHNOLOGY LADKRABANG
- BACHELOR OF SCIENCE KING'S MONGKUT INSTITUTE OF TECHNOLOGY NORTH BANGKOK
- DIPLOMA PROGRAM FOR MANAGEMENT KELLOGG – NORTHWESTERN UNIVERSITY, UNITED STATE OF AMERICA
  Certificate:

  - Microsoft Certified professional (MCP)
  - Microsoft Certified Systems Administrator (MSCA)
  - Microsoft Certified Systems Engineer (MSCE)
  - Cisco Certified Network Associate (CCNA)
  - Certificate of CompTIA Security+
  - Certified Technical training CTT+
  - Certified Ethical Hacker
  - Certified Hacking Forensic Investigator
  - Certified Wireless Network Administrator
  - Certified Wireless Security Professional

จำนวนชั่วโมงในการฝึกอบรม : 5 วัน (30 ชั่วโมง)

กำหนดการอบรม : ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

ค่าลงทะเบียนอบรม : ท่านละ 25,500 บาท (ราคารวมภาษีมูลค่าเพิ่มแล้ว)
** สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

สถานที่ฝึกอบรม :
    สถาบันพัฒนาบุคลากรแห่งอนาคต
    เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
    ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

วิธีการการสำรองที่นั่ง :
    ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
    โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887
    โทรสาร: 0 2644 8110
    Website: www.career4future.com
    E-mail: training@nstda.or.th