TEC017: Penetration Testing with Kali Linux (PWK)

Overview:

Penetration Testing with Kali Linux is designed for IT Professionals who are new to Kali Linux. This course will actively engage students in task focused activities, lab-based knowledge checks, and facilitative discussions to ensure maximum skill transfer and retention. In addition, GUI-based Environment will be featured to build on the student's existing technical knowledge, while command line concepts will be introduced to provide a foundation for students planning to become full time kali Linux expert. Moreover, the course will also prepare students for the Offensive Security Certified Professional (OSCP) exam, which typically proceeds the PWK course. Students should be familiar with Linux command line, common networking terminology, and basic Bash/Python scripting prior to attempting this course.

Audience:

Ethical Hackers, Penetration Testers, Security Analysts, Security Engineers, Network Server Administrators, Firewall Administrators, Security Testers, System Administrators, and Risk Assessment Professionals

Prerequisites:

Penetration Testing with Kali Linux is a foundational course, but still requires students to have certain knowledge prior to attending the online class. A solid understanding of TCP/IP, networking, and reasonable Linux skills are required. Familiarity with Bash scripting along with basic Perl or Python is considered a plus.

Course objectives:

After completing this course, the attendees will;

- Gain insight into the offensive security field, which will expand awareness for the need of real-world security solutions.
- Learn to implement various reconnaissance techniques, identify various attack vectors and identify various post exploitation techniques.
- To make you aware of the hazards of malicious activities perforated by the Black-hat hackers.
- This Kali Linux Training will give you in-depth knowledge about how actual hacking is done, and how to test an environment and its reliability which people term as highly secure.

Course Outline:

Topics and hands-on exercises for the course include:

- Introduction to Kali
- Information Gathering
- Port Scanning
- Sniffing/Spoofing/Main-in-the-Middle
- Buffer Overflow
- Working with Exploits
- Exploit Framework/Metasploit
- Password Attacks
- DoS Attack
- Web Application Attacks
- Trojan Horses
- Rootkits
- Penetration Testing Techniques

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 35,000 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