Certified Ethical Hacker, Part 3 of 8: Threats and System Hacking

page 1

Meet the expert: Rafiq Wayani has extensive experience including more than 20 years in IT as Systems Architect, Software Engineer, DBA, and Project Manager. Wayani has instructed in a variety of technical areas, has designed and implemented network and information systems, and is certified across a wide range of platforms and systems including Microsoft Solutions Developer, Systems Engineer, Application Developer, Database Administrator, Trainer; Novell Netware Administrator and Engineer; Master Certified Netware Engineer; and A Certified.

Prerequisites: To get the most out of this course, this course assumes that you have a good working knowledge of Linux and Windows based networking environments. It also assumes that you have experience with managing a network, have worked with networking hardware such as switches & routers, are familiar with MS Active Directory (AD) Domain based authentication, know how to work with command-line utilities, and understand the basics of Web Server environments.
Many of the demonstrations in this course use the Windows 7 and Kali Linux operating systems which can be downloaded free from the respective sites. All of the demonstrations are created in a virtual environment using Oracle VirtualBox and VMware vSphere 6.

Runtime: 01:40:55

Course description: This course narrows in on how to identify threats both external and internal. Perhaps one of the employees of the business uses a very weak password and this is a security threat that a dictionary attack tool can rapidly find. It then covers how to gain information or "footprinting" on a target of ethical hacking. It shows how to scan and also to mitigate scans to acquire information about weak points and then explains diagramming your system from a hacking perspective. This course is part of a series covering EC-Council's Certified Ethical Hacker (CEH).

Course outline:

Threats
- Introduction
- Threats
- Demo: Using Google
- Internet Searches
- Demo: Google Hacking
- Demo: Other Databases
- Summary

Scanning
- Introduction
- Environment Evaluation
- Environment
- Demo: Zenmap and NMap
- Summary

Scanning Demo
- Introduction
- Mitigate Scans
- Honeypot
- Summary

Enumeration
- Introduction
- Enumeration
- Demo: Enumeration Script
- Enumeration Cont.
- Demo: PowerShell Enumeration
- Protecting Against Enumeration
- Summary

Enumeration Demo
- Introduction
- Demo: Enumerating Classes
- Demo: Enumeration Tools
- Summary

System Hacking
- Introduction
- System Hacking
- Hacker Goals
- Methods of Attack
- Summary

System Hacking Demos
- Introduction
- Demo: Password Attack
- Demo: Dictionary Passwords
- Demo: NetCat
- Summary