Certified Ethical Hacker, Part 5 of 8: Sessions and Web Servers

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: 01:41:34

Course description: Given their centrality in operations of most businesses, Websites represent tempting and low-hanging fruit for hackers. Experienced systems architect, software engineer and cybersecurity expert Rafiq Wayani reveals how both session hacking and the hacking of entire web servers have become all too commonplace. Wayani discusses the latest detection tools, counter measures and penetration testing you will need to thwart these attacks. This course is part of a series covering EC-Council's Certified Ethical Hacker (CEH).

Course outline:

Session Hijacking Concepts
- Introduction
- Session Hijacking
- Session Hijacking Diagram
- Session Hijacking Cont.
- Summary

App Level Session Hijacking
- Introduction
- Application Level Hijacking
- Web Services
- Summary

Network Level Hijacking
- Introduction
- Network Level Hijacking
- Models
- Summary

Session Hijacking Tools
- Introduction
- Network Level Hijacking
- Demo: Session Hijacking Tools
- Summary

Session Hijack Countermeasures
- Introduction
- Session Hijack Countermeasures
- Countermeasures Cont.
- Summary

Session Hijack Pentest
- Introduction
- Session Hijack Pentest
- Session Hijack Pentest Cont.
- Summary

Web Server Concepts
- Introduction
- What's Happening
- HTTP Request Processing in IIS
- Summary

Web Server Attacks
- Introduction
- Web Server Attacks
- Demo: Netsparker
- Summary

Web Server Attack Methodology
- Introduction
- Web Server Attack Methodology
- Demo: Netsparker
- Web Server Attack Methodology
- Demo: WinHTTrack
- Summary

Web Server Attack Tools
- Introduction
- Web Server Attack Tools
- Demo: Passivetotal
- Demo: HTTPRecon
- Summary

Web Server Countermeasures
- Introduction
- Web Server Countermeasures
- 18-Year-Old Vulernerability
- Server O/S
- Demo: End-of-Life Support
- Web Server Countermeasures
- Demo: Locking Down Servers
- Web Server Countermeasures
- Summary

Web Server Patch Management
- Introduction
- Web Server Patch Management
- Patch Management Cont.
- Summary

Web Server Security Tools
- Introduction
- Web Server Security Tools
- Demo: Cache
- Summary

Web Server Penetration Testing
- Introduction
- Web Server Penetration Testing
- Demo: Pen Test Tools
- Web Server Pen Testing
- Summary