Certified Ethical Hacking: Advanced

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: 06:25:50

Course description: Certified Ethical hacking Advanced Master Course

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

Web Application Concepts
- Introduction
- Most Exposed & Least Protected
- Exposure & Protection Cont.
- Summary

Web Application Threats
- Introduction
- Web Application Threats
- Application Replays Script
- Email Vector
- Decoded Attack Sequence
- Verbose and Blind
- SQL Injection
- Database Driven Page
- Piggybacking with UNION
- Enumerate All Tables
- Subquery Enumerates Columns
- Select Data from the Column
- Summary

Web App Hacking Methodology
- Introduction
- Web App Hacking Methodology
- Demo: Netsparker
- Web App Hacking Methodology
- Summary

Web Application Hacking Tools
- Introduction
- Web Application Hacking Tools
- More Hacking Tools
- Summary

Web App Countermeasures
- Introduction
- Countermeasures
- How to Protect Yourself
- Summary

Web App Security Tools
- Introduction
- Demo: Kali, Nmap, & Nessus
- Demo: Openwall, pof, & WireShark
- Demo: Netcraft, Yersinia, & PuTTY
- Demo: Cain & Abel and Kismet
- Demo: hping and Secapps
- Summary

Web Application Pen Testing
- Introduction
- Demo: Veracode
- Demo: Shodan and Arachni
- Demo: Aircrack-ng, AppScan, & Nikto
- Demo: WebScarab, Paterva, & Ironwasp

(Continued on page 2)

Certified Ethical Hacking: Advanced

- Demo: Metasploit & WireShark
- Demo: w3af, Impact Pro, and Kali
- Demo: Netsparker, Nessus & Portswigger
- Demo: Zed Attack & Acunetix
- Demo: BeyondTrust, SQLNinja, & BeEF
- Demo: Dradis & Ettercap
- Summary

SQL Injection Concepts
- Introduction
- SQL Injection (SQLi)
- How Does SQLi Work?
- Summary

SQL Injection Types
- Introduction
- Types of SQLi
- How Does SQLi Work?
- Summary

SQLi Attack Methodology
- Introduction
- Application Security Risks
- OWASP Top 10
- Summary

SQLi Tools
- Introduction
- SQLi Tools
- Demo: sqlmap
- Demo: SQL Ninja
- Demo: safe3
- Summary

SQLi Evasion Techniques
- Introduction
- SQLi Evasion Techniques
- SQLi Evasion Techniques Cont.
- Summary

SQLi Countermeasures
- Introduction
- SQLi Countermeasures
- Demo: Web Application Firewall
- SQLi Countermeasures
- Summary

Wireless Networking Concepts
- Introduction
- Wireless Networking Concepts
- Directional Antennae
- Wireless Networking Concepts
- Omnidirectional Antennae
- Summary

Wireless Encryption
- Introduction
- Wireless Encryption
- Demo: WPA2
- Summary

Wireless Threats
- Introduction
- Wireless Threats
- Rogue APs
- Wireless Threats
- Summary
- Wireless Hacking Methodology
- Wifite
- Wireless Hacking Methodology
- Wifiphisher
- Summary

Wireless Bluetooth Hacking
- Introduction
- Bluetooth: Basics
- Bluetooth Hacking
- Bluetooth Security
- Bluetooth Hacking Tools
- Summary

Wireless Countermeasures
- Introduction
- Wireless Countermeasures
- Demo: CIRT.net Passwords
- Wireless Countermeasures
- Demo: Linksys Settings
- Summary

IDS, Firewalls, and Honeypots
- Introduction
- Intrusion Detection System
- Network-Based IDS
- Host-Based IDS
- Intrusion Detection Techniques
- Summary

Evading IDS
- Introduction
- Evading IDS
- IDS Diagram
- Summary

Evading Firewalls
- Introduction
- Types of Firewalls
- Firewall Diagram
- Evading Firewalls
- Spoofing Diagram
- Evading Firewalls
- Source Routing Diagram
- Evading Firewalls
- Summary

Evading Firewall Tools
- Introduction
- Evading Firewall Methods
- Demo: Loki
- HTTP Tunneling Diagram
- Evading Firewall Tools
- Demo: Traffic IQ Professional
- Evading Firewall Tools
- Demo: Evading Firewall Tools
- Your Freedom Diagram
- Demo: More Evading Tools
- Summary

Detecting Honeypots
- Introduction
- Detecting Honeypots
- Detecting Honeypots Cont.
- Summary

IDS Evasion Countermeasures
- Introduction
- Attacker Creativity
- Network Monitor
- Insertion
- Attacker Creativity
- Summary

IDS Penetration Testing
- Introduction
- IDS/Firewall Pen Testing
- Penetration Tesing Cont.
- Summary

Intro to Cloud Computing
- Introduction
- Intro to Cloud Computing
- Cloud Computing Diagram
- Intro to Cloud Computing
- Pizza as a Service
- Intro to Cloud Computing
- Summary

Cloud Computing Threats
- Introduction
- Cloud Computing Threats
- Cloud Computing Threats Cont.
- Summary

Cloud Computing Attacks
- Introduction
- Cloud Computing Attacks
- Cloud Computing Attacks Cont.
- Summary

Cloud Security
- Introduction
- Cloud Security
- Cloud Security Cont.
- Summary

Cloud Security Tools
- Introduction
- Demo: Cloud Security
- Demo: Cloud Security Tools
- Summary

Cloud Penetration Testing
- Introduction
- Cloud Penetration Testing
- Cloud Pen Testing Cont.
- Summary

2014: The Year of Encryption
- Introduction
- 2014: The Year of Encryption
- The Year of Encryption Cont.
- Summary

Case Study: Heartbleed
- Introduction
- Demo: The Heartbleed Bug
- Demo: The Heartbleed Bug Cont.
- Summary

Case Study: POODLEbleed
- Demo: POODLEbleed Cont.
- Summary

Cryptography Concepts
- Introduction
- Cryptography Concepts
- Cryptography Concepts Cont.
- Summary

Encryption Algorithms
- Introduction
- Encryption Algorithms
- Encryption Algoritms Cont.
- Summary

Public Key Infrastructure
- Introduction
- Public Key Infrastructure
- PKI Cont.
- Summary

Email Encryption
- Introduction
- Demo: Email Encryption
- Demo: Email Encryption Cont.
- Summary

Disk Encryption
- Introduction
- Disk Encryption
- Disk Encryption Cont.
- Summary

Cryptography Attacks
- Introduction
- Cryptography Attacks
- Cryptography Attacks Cont.
- Summary

Security Tools
- Introduction
- Demo: CrypTool
- Demo: Cipher Tools
- Demo: Matasano Challenges
- Summary