Certified Ethical Hacker, Part 7 of 8: Wireless Networks and Firewalls

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: 01:44:02

Course description: Much as mobile platforms have changed society as a whole, they have also radically altered the battlespace between hackers and the security professionals dedicated to stopping them. In this session, Rafiq Wayani will discuss how hackers are using wireless networks to attack and evade traditional security tools, intrusion detection systems, firewalls, and honeypots. This course is part of a series covering EC-Council's Certified Ethical Hacker (CEH).

Course outline:

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
- Introduction
- 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