Certified Ethical Hacker, Part 4 of 8: Malware and Social Engineering

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: 02:11:21

Course description: There are many different types of Malware from trojans and worms to viruses and backdoors. Learning about how each threat is different is key and about how to mitigate it. Examples will be shown with Wireshark and how to interact with Packets. Also the human element of Ethical Hacking will be covered. Perhaps a company is very good in network security but lacking in physical security. This is an area that social engineering can come into play. How do you case an establishment and look for week points in the human element? And also how can you attempt to mitigate these threats. This course is part of a series covering EC-Council's Certified Ethical Hacker (CEH).

Course outline:

Trojans and Backdoors
- Introduction
- Trojans & Backdoors
- Trojan
- Virus & Worm
- Summary

Trojans and Backdoors Demo
- Introduction
- Demo: Creating a Backdoor
- Demo: Using a Backdoor
- Summary

Viruses
- Introduction
- Viruses
- Virus Types
- Things to Remember
- Summary

Viruses Demo
- Introduction
- Demo: TeraBIT Virus Maker
- Demo: Virus
- Summary

Worms
- Introduction
- Worms
- Not Like a Virus
- Mitigating Worms
- Summary

Worms Demo
- Introduction
- Demo: Internt Worm Maker Thing
- Demo: Worm Settings
- Demo: Inside the Worm
- Summary

Sniffing
- Introduction
- Sniffing
- Protecting Your Network
- Demo: Sniffing
- Demo: Wireshark
- Demo: Spoofing
- Demo: Manipulate Source
- Summary

Social Engineering
- Introduction
- Social Engineering
- Means of Social Engineering
- Social Engineering Requirement
- Summary

Social Engineering Techniques
- Introduction
- Social Engineering Techniques
- More Techniques
- Even More Techniques
- Summary

Tech Attacks Countermeasures
- Introduction
- Soc. Engineering: Tech Attacks
- Countermeasures
- Summary

DOS Attacks
- Introduction
- Denial of Service (DOS) Attack
- DOS Attack Targets
- Demo: DOS Attack
- Summary