This course includes an overview of the various types of wireless (802.11) networks, available encryption security systems (WEP, WPA, and WPA2), and how to use open-source tools to hack and crack these vulnerable wireless (WiFi) networks.

Since their introduction in 1999, wireless networks have been rapidly expanding in their usage and availability. Unfortunately, many people believe these wireless networks are designed as a secure solution for sharing data, but this is rarely the case. In this course, you will gain a deeper understanding of the WEP, WPA, and WPA2 wireless security protocols, and how to exploit their vulnerabilities in order to gain access to any wireless network during a penetration test. You will use this information to increase the security of your networks and to implement a better defensive security posture to prevent an attacker from accessing your networks.

What Other Students Are Saying About This Course:

- **Just completed the course as a newbie and followed all steps exactly and was able to complete everything!! Thank you Jason!!!! (Stephanie, 5 stars)**
- **Great course that goes into detail of how vulnerable Wireless really is... would definitely recommend to anyone who wants to go into InfoSec or Network Security. (Matthew, 5 stars)**
- **Great course. Step by step instructions, good quality audio and video lectures. Easy to understand instructor is very important, especially when he explains everything in detail. (Alisher, 5 stars)**