HACKINGPOINT

Check Point SOFTWARE TECHNOLOGIES LTD.

WiFi Hacking

2 days class

Get Certified

If you want to learn how to understand and compromise Wi-Fi networks, this is your course. Learning modern Wi-Fi hacking can be a pain. There is lots of outdated material for technologies we rarely see deployed in the real world anymore. Numerous tools overly rely on automation, and leave you wondering when they don't work, because neither the fundamentals nor underlying attack is understood. Even worse, some popular attacks will rarely if ever work in the real world. If you want to really understand what's going on, and master the attacks in such a way that you can vary them when you encounter real world complexities, this course will teach you what you need to know. We've been pen testing Wi-Fi networks for nearly two decades, and have built some popular Wi-Fi hacking tools such as Snoopy and Mana. This course is highly practical, with concepts taught through theory delivered while your hands are on the keyboard, and semi-self-directed practicals at the end of each section to reinforce the learning. The course is hosted in a "Wi-Fi in the cloud" environment we invented several years ago, which means no more fiddling with faulty hardware or turning the classroom into a microwave.

LEARNING OBJECTIVES

How Wi-Fi hacking fits into wider attack or defence objectives Important physical and low level RF concepts and how to reason through/debug strange situations Understanding how monitor mode works, when to use or not use it, and practical examples of what to do with collected frames or data Grokking the WPA2 4-way handshake and the numerous ways of recovering PSKs and what do with them

First looks at attacking WPA3's Dragonfly handshake with downgrades Grokking EAP & EAP vulnerabilities relating to certificate validation, tunnelled mode key derivation and how to practically attack them with downgrades, relays and manipulating state

WHY SHOULD PEOPLE ATTEND THE COURSE?

Take this course if you want to learn Wi-Fi fundamentals well enough to adjust approaches when the basics aren't working. Take this course to learn about new Wi-Fi security protocols like WPA3 and OWE. Take this course to learn about newer Wi-Fi attacks like EAP tunnelling (sycophant), LootyBooty (EAP-GTC downgrade), PMKID cracking and more.

TAKEAWAYS:

Modern Wi-Fi hacking How to think about and adjust approaches when facing obstacles New approaches and tooling

WHO SHOULD TAKE THIS COURSE:

This course is for anyone who wants to understand how to attack and defend Wi-Fi networks. It's an offensive course and has obvious benefits for pentesters and red teamers, however it's also essential for disabusing defenders of false notions of security as well as what defences have a meaningful impact.

REQUIREMENTS:

A laptop with internet access and a modern browser such as Chrome/Firefox