Hardware requirements

We will need the following hardware to set up the wireless lab:

- **Two laptops with internal Wi-Fi cards**: We will use one of the laptops as the victim in our lab and the other as the penetration tester's laptop. Though almost any laptop would fit this profile, laptops with at least 3 GB RAM are desirable. This is because we may be running a lot of memory-intensive software in our experiments.
- **One wireless adapter (optional)**: Depending on the wireless card of your laptop, we may need a USB Wi-Fi card that can support packet injection and packet sniffing, which is supported by Kali. The best choice seems to be the Alfa AWUS036H card from Alfa Networks, as Kali supports this out of the box. This is available on `www.amazon.com` for a retail price of £18 at the time of writing. An alternative option is Edimax EW-7711UAN, which is smaller and, marginally, cheaper.
- **One access point**: Any access point that supports WEP/WPA/WPA2 encryption standards would fit the bill. I will be using a TP-LINK TL-WR841N Wireless router for the purpose of illustration in this book. You can purchase it from `www.amazon.com` for a retail price of around £20 at the time of writing.
- **An internet connection**: This will come in handy for performing research, downloading software, and for some of our experiments.

Software requirements

We will need the following software to set up the wireless lab:

- **Kali**: This software can be downloaded from the official website located at `http://www.kali.org`. The software is open source, and you should be able to download it directly from the website.
- **Windows XP/Vista/7/10**: You will need any one of Windows XP, Windows Vista, Windows 7, or Windows 10 installed on one of the laptops. This laptop will be used as the victim machine for the rest of the book.