

13.4 Hacking Wi-Fi

Wi-Fi is also another obvious target for attack. Given its easy accessibility, it is likely that any attacker will at least attempt to breach your Wi-Fi. There are several common attacks you should be familiar with. Each of these can present a danger to your network.

- **Jamming:** This involves simply attempting to jam the Wi-Fi signal so that users cannot get on the wireless network. This is essentially a denial of service attack on the wireless access point.
- **De-authentication:** This is sending a de-authentication or logoff packet to the wireless access point. The packet will spoof the user's IP address. This can be done in order to trick the user into then logging in to the rogue access point.
- **WPS attack:** Wi-Fi Protected Setup (WPS) uses a PIN to connect to the wireless access point. The WPS attack attempts to intercept that PIN in transmission, connect to the WAP, and then steal the WPA2 password.
- **Cracking the password:** Actually, breaking the encryption is usually not something that is likely to succeed. However, cracking bad Wi-Fi passwords is certainly possible.