# Article information:

GitHub - ankit0183/Wifi-Hacking: Cyber Security Tool For Hacking Wireless Connections Using Built-In Kali Tools. Supports All Securities (WEP, WPS, WPA, WPA2/TKIP/IES)
<https://github.com/ankit0183/Wifi-Hacking>

# Article summary:

1. Wifi-Hacking.py is a cyber security tool for hacking wireless connections using built-in Kali tools. It supports all securities (WEP, WPS, WPA, WPA2/TKIP/IES).

2. Features and contains of the tool include starting monitor mode, stopping monitor mode, scanning networks, getting handshake, creating wordlist, installing wireless tools, WPS networks attacks, scanning for WPS networks and cracking handshake with rockyou.txt or wordlist.

3. The creator of the tool is Ankit Kanojiya and it has been tested on Kali Linux, BlackArch Linux, Ubuntu, Kali Nethunter, Termux (Rooted Devices), Parrot OS.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article appears to be reliable in terms of its content as it provides detailed information about the features and capabilities of the tool as well as instructions on how to install it on different operating systems. However, there are some potential biases that should be noted. Firstly, the article does not provide any evidence to support its claims about the effectiveness of the tool in hacking wireless connections or any other security measures that may be in place. Additionally, there is no mention of any possible risks associated with using this tool or any counterarguments that could be made against its use. Furthermore, there is a promotional element to the article as it encourages readers to donate money to the creator if they find it useful and also includes his contact details for further discussion. Finally, while both sides of an argument are not presented equally in this article – i.e., those who would argue against using such a tool – this could be seen as a limitation rather than bias since it is focused solely on promoting the use of this particular tool rather than providing an unbiased overview of all available options for hacking wireless connections.

# Topics for further research:

* Wireless connection hacking risks
* Alternatives to wireless connection hacking
* Security measures for wireless connections
* Legality of wireless connection hacking
* Potential consequences of wireless connection hacking
* Ethical considerations of wireless connection hacking

# Report location:

<https://www.fullpicture.app/item/1f41c114c0626fd162517767264a0cf5>