By Robert McMillan, PCWorld.com

For US$34, a new cloud-based hacking service can crack a WPA (Wi-Fi Protected Access) network password in just 20 minutes, its creator says.

Launched Monday, the WPA Cracker (https://www.wpacracker.com/) service bills itself as a useful tool for security auditors and penetration testers who want to know if they could break into certain types of WPA networks. It works because of a known vulnerability in Pre-shared Key (PSK) networks, usually used by home and small-business users.

To use the service, the tester submits a small ˝handshake˝ file that contains an initial back-and-forth communication between the WPA router and a PC. Based on that information, WPA Cracker can then tell whether the network seems vulnerable to this type of attack or not.

The service was launched by a well-known security researcher who goes by the name of Moxie Marlinspike. In an interview, he said that he got the idea for WPA Cracker after talking to other security experts about how to speed up WPA network auditing. ˝It`s kind of a drag if it takes five days or two weeks to get your results,˝ he said.

Hackers have known for some time that these WPA-PSK networks are vulnerable to what`s called a dictionary attack, where the hacker guesses the password by trying out thousands of commonly used passwords until one finally works. But because of the way WPA is designed, it takes a particularly long time to pull off a dictionary attack against a WPA network.

Because each WPA password must be hashed thousands of times, a typical computer can guess perhaps just 300 passwords per second, while other password crackers can process hundreds of thousands of words per second. That means that the 20-minute WPA Cracker job, which runs 135 million possible options, would take about five days on a dual-core PC, Marlinspike said. ˝That has really stymied efforts of WPA cracking,˝ he said.

WPA Cracker customers get access to a 400-node computing cluster that employs a custom dictionary, designed specifically for guessing WPA passwords. If they find the $34 price tag too steep, they can use half the cluster and pay $17, for what could be a 40-minute job. Marlinspike declined to say who operates his compute cluster.

The attack will work if the network`s password is in Marlinspike`s 135 million-phrase dictionary, but if it`s a strong, randomly generated password it probably won`t be crackable.

The service could save security auditors a lot of time, but it will probably make it easier for senior management to understand the risks they`re facing, said Robert Graham, CEO of penetration testing company Errata Security. ˝When I show this to management and say it would cost $34 to crack your WPA password, it`s something they can understand,˝ he said. ˝That helps me a lot.˝