Daniel Hautzinger
Computing and Information Sciences

Abstract

This project conducted a careful investigation into the capabilities of the Hak5 Wifi Pineapple Mark VII, which is a commercially available security and testing apparatus for wireless networks. This device has been used by cybersecurity engineers and companies to audit the networks of many different businesses. A key question of this investigation was whether the device is suitable for use in classroom environments. The risks, side effects, and propriety of the Pineapple were of particular focus. This project also investigated the ethical and legal implications that might arise from use or even casual reception of signal. The investigation concluded that the Wifi Pineapple Mark VII is only suitable for carefully supervised or monitored use. Regardless of the user's intent, the impact and damage that this high-risk tool can cause to nearby devices makes it much too dangerous to use in a classroom environment.

Motivation/Initial Selection

The initial idea behind this project was to find a way to teach networking and the different facets of security in networking. Research was conducted into the different tools and techniques that could be used in a classroom setting. Eventually, the Hak5 Wifi Pineapple Mark VII was chosen.

The Wifi Pineapple is a device that is used by many cybersecurity and networking companies to audit networks. It is a tool that is easy to learn and use and also provides detailed information about network security. The device is also extremely easy to assemble and access. There are many tutorials[1] that detail what each and every feature of the Pineapple is capable of and how to use those features.

Selected Tool

The Hak5 Wifi Pineapple is a tool that many would be cautious to use. While it is a useful tool to learn about networking, the Pineapple and its abilities raise many ethical and legal concerns. Some of the features of the Pineapple, when used incorrectly, would be considered illegal.

Wifi Pineapple Logo

***Figure 1**: Hak5 Wifi Pineapple Mark VII kit*

The Wifi Pineapple is particularly popular is what is known as coffee shop attacks. A coffee shop attack is where the user of the Pineapple is able to trick multiple users into thinking they are connecting to a certain wifi, such as a coffee shop wifi, when they are actually connecting to the Pineapple. This allows the Pineapple user to collect login credentials and other information.

One feature that the Wifi Pineapple boasts in the ability to spoof Wifi networks. This allows the Pineapple to disguise itself as a known wifi network and force wifi users to connect to the Pineapple wifi. This then allows for the user of the Pineapple to target the users connected to the spoofed network.This raises legal concerns[2] as someone inexperienced in the Pineapple could gather data through illegal means from the connections.

Figure 2: Fully assembled Hak5 Wifi Pineapple

Observations

The Wifi Pineapple is extremely dangerous when used improperly. During the investigation a Iphone was connected to the Pineapple. The Pineapple allows the user to choose the name of the network. There is a particular name that causes the network of the phone to crash. The phone in the investigation was only fixed after a factory reset was done. This allowed for all network settings on the Iphone to be completely reset. This is one of many dangerous things that the Pineapple can do. The amount of data and information that it can collect can very easily become illegal because of the way that it was obtained. In untrained hands the Pineapple is an extremely dangerous tool, bordering on being classified as a weapon.

Conclusion

The Hak5 Wifi Pineapple is much to dangerous of a tool to safely use in a classroom setting. The severity of the risks that are taken would require a high amount of supervision in order to ensure that the usage is kept to a legal level. The kind of class that would use this as a learning tool would consist of at least twenty people, and the risks from the large amount of people far outweigh the reward of using the Wifi Pineapple. University officials are rightly concerned about allowing the Wifi Pineapple to be used in the community. The Wifi Pineapple should only be used in small classes of advanced students. The class should also be heavily monitored and taught in a restricted environment. While the Hak5 Wifi Pineapple is an extremely useful tool for a professional, the knowledge to be gained from this forbidden fruit is much to dangerous for an inexperienced student.

References

1. https://docs.hak5.org/hc/en-us/categories/360004116253-WiFi-Pineapple-Mark-VII
2. https://us.norton.com/internetsecurity-malware-ip-spoofing-what-is-it-and-how-does-it-work.html

Acknowledgements

Thanks to the NSF EPIC Scholarship (Grant Award Number 1564855) and the Valparaiso University Department of Computing and Information Sciences for financial and hardware support. Thanks, also, to my project advisor Professor Nicholas S. Rosasco, DSc.