**LM 6. Wireless Network Security Tools**

1. **LM6. Student Learning Outcomes**

After completing this module, a student will be able to:

* Describe the functionalities of built-in commonly used network utilities tools for Windows and Mac OS.
* Describe the functionalities of WLAN discovery tools such as NetStumbler, InSSIDer, Kismet and HeatMapper.
* Describe the functionalities of network protocol analyzing tools, such as Aircrack-ng, Wireshark and Airshark.
* Describe penetration testing. Discuss the penetration testing tools such as metasploit and SARA.

1. **LM6. Learning Material & Study Guide**

* Describe the functionalities of built-in commonly used network utilities tools for Windows and Mac OS.
* Window OS: <http://techgenix.com/top-11-networking-commands/>
* Mac OS: <https://support.apple.com/en-us/HT202790> (optional)
* Describe the functionalities of WLAN discovery tools such as NetStumbler, InSSIDer, Kismet and HeatMapper.

- NetStumbler (Windows OS): <http://stumbler.net>

- InSSIDer (free on Linux): <https://www.metageek.com/products/inssider/>

- Kismet: <https://www.kismetwireless.net>

- Wireshark: <https://www.wireshark.org>

- HeatMapper (WLAN site survey tool): <https://www.ekahau.com/products/heatmapper/overview/>

* Describe the functionalities of network protocol analyzing tools, such as Aircrack-ng and Wireshark.
* Aircrack-ng: <https://www.aircrack-ng.org>
* Wireshark: <https://www.wireshark.org>
* Describe penetration testing. Discuss the penetration testing tools such as metasploit and SARA.
* Penetration test: <https://www.coresecurity.com/content/penetration-testing>
* Metasploit: <https://metasploit.com>
* SARA: <https://www.darknet.org.uk/2008/11/sara-security-auditors-research-assistant-network-analysis-tool/>