**Mobile Communications Security Assessment**

**Conducted by Brendan Murphy**

**3/9/2019**

Contents

[1. Executive Summary 2](#_Toc460775246)

[2. Test Parameters 2](#_Toc460775247)

[3. Targets 2](#_Toc460775248)

[4. Analysis 3](#_Toc460775249)

[5. Appendix – Documentation 5](#_Toc460775250)

# Executive Summary

The purpose of this document is to evaluate the security of Mobile Communications on a select network.

The security of the mobile communications network 'GiantHavoc' is strong and has no support for weak encryption protocols such as WEP or WPA. The network also shows extremely low network noise, this could be an ancillary benefit of a recently upgraded router from the Starry internet provider. The security flaws of the network are primarily a weak network passcode that can be hacked using brute force tactics, to mitigate this I recommend replacing with a more complex password as soon as possible. Lastly, the network is vulnerable to Man in the Middle (MitM) attacks. In order to prevent this type of attack I recommend that the network adopt a more secure encryption protocol available in the settings of the newly installed router.

# Test Parameters

The Objective of this evaluation is to conduct passive and active reconnaissance on the Mobile Communications of a selected network. The Scope of this evaluation is **wlan0. wlan0** is a wireless network operating on 802.11. This evaluation includes Passive Reconnaissance and Active Reconnaissance evaluation techniques. Wireless Analysis tools include:

* **Kismet**
* **WireShark**
* **Aircrack**

# Targets

The Scope of the evaluation is as follows:

**Information Gathering**

* 1. wlan0

# Analysis

Table 1: Passive Reconnaissance

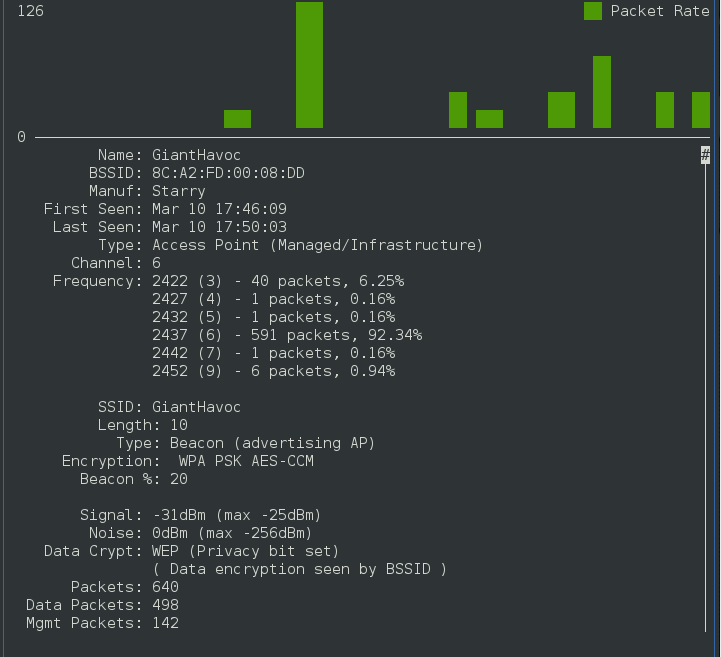
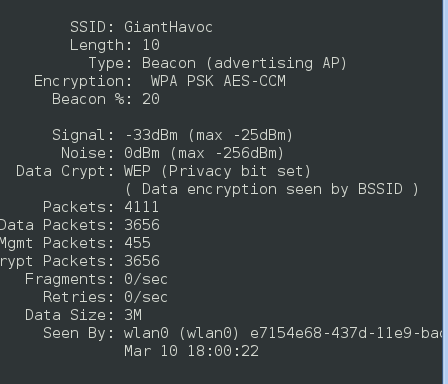
|  |  |  |
| --- | --- | --- |
| **COMMUNICATIONS COMPONENT** | **DESCRIPTION** | **EVIDENCE** |
| **WiFi Network Channel** | **6** | **Appendix A** |
| **# of WiFi Packets Network is Processing** | **126 packet rate** | **Appendix A** |
| **Channels External WiFi Networks are Operating On** | **1, 2, 4, 6, 11** | **Appendix A** |
| **# of WiFi Networks implementing Encryption** | **36** | **Appendix A** |
| **Access Point Frequencies** | **2412, 2437, 2462** | **Appendix A** |
| **Access Point Type of Traffic** | **Beacon** | **Appendix A** |
| **Access Point Encryption** | **WPA PSK AES-CCM** | **Appendix A** |
| **Access Point Signal** | **-33dBm (max -25dBm)** | **Appendix A** |
| **Access Point Noise** | **0dBm (max -256dBm)** | **Appendix A** |
| **Access Point Packets** | **4111** | **Appendix A** |
| **Access Point Data Packets** | **3656** | **Appendix A** |
| **Access Point Management Packets** | **455** | **Appendix A** |
| **Access Point Crypt Packets** | **3656** | **Appendix A** |
| **Access Point Fragments** | **0/sec** | **Appendix A** |
| **Access Point Retries** | **0/sec** | **Appendix A** |
| **Access Point Data Size** | **3m** | **Appendix A** |

Table 2: Active Reconnaissance

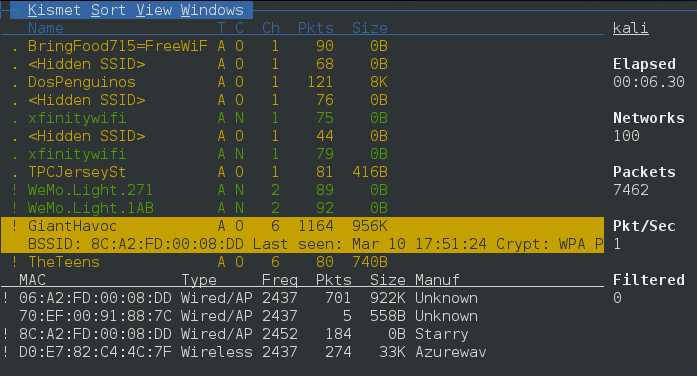
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VULNERABILITY** | **DESCRIPTION** | **RISK ANALYSIS** | **DOCUMENTATION** | **RECOMMENDATION** |
| **Weak Access Point Encryption\*** | **The communications on this channel does not support weak encryption protocols (e.g. WEP, WPA)** | **Low** | **Appendix B** | **None at this time** |
| **Low Signal-to-Noise Ratio\*** | **No** | **Low** | **Appendix B** | **Very low network noise** |
| **Communications Interference\*\*** | **Yes** | **Medium** | **Appendix B** | **Kill these processes to reduce interference** |
| **Weak WPA2 Authentication\*\*** | **The WLAN implements a weak shared passcode. The communications on this network is subject to a brute force dictionary attack.** | **Medium** | **Appendix B** | **Passcode should be strengthened to avoid a brute force attack** |
| **Network Allows for MiTM\*\*\*** | **Yes** | **High** | **Appendix B** | **Network security should be improved to reduce the opportunity of MiTM attacks** |

**\*Detected via Kismet  
\*\*Detected via Aircrack  
\*\*\*Confirmed via WireShark**

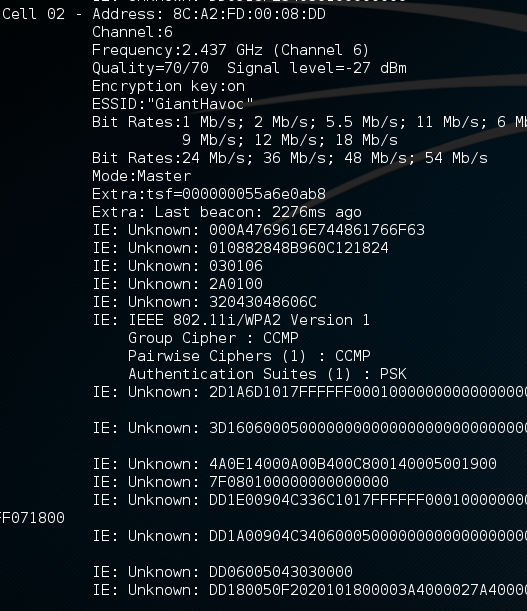
# Appendix – Documentation

** **

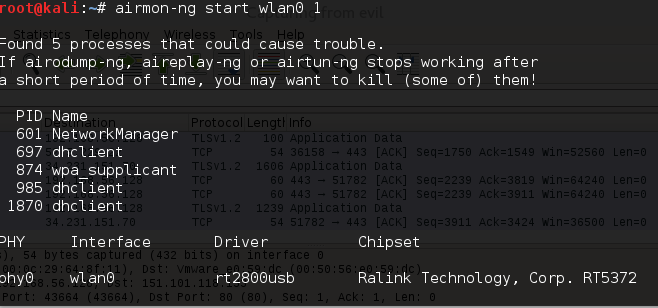
**Appendix A: Wifi network 'GiantHavok' details**

****

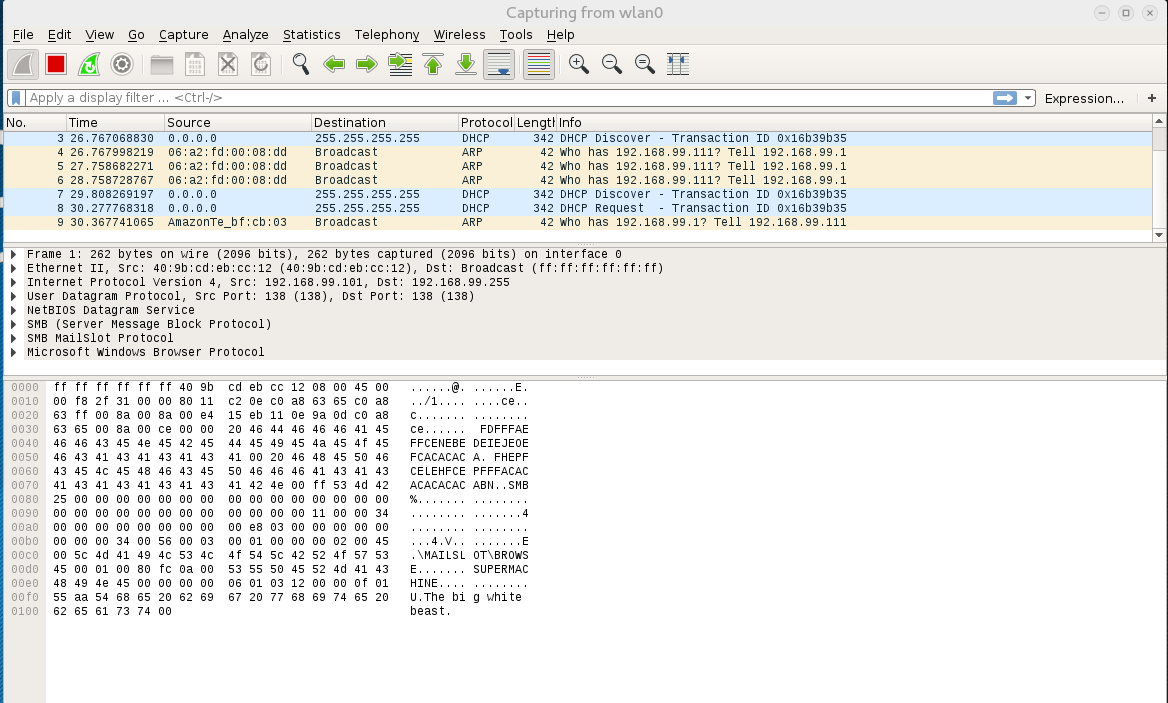
**Appendix A: Wifi network 'GiantHavok' details**

****

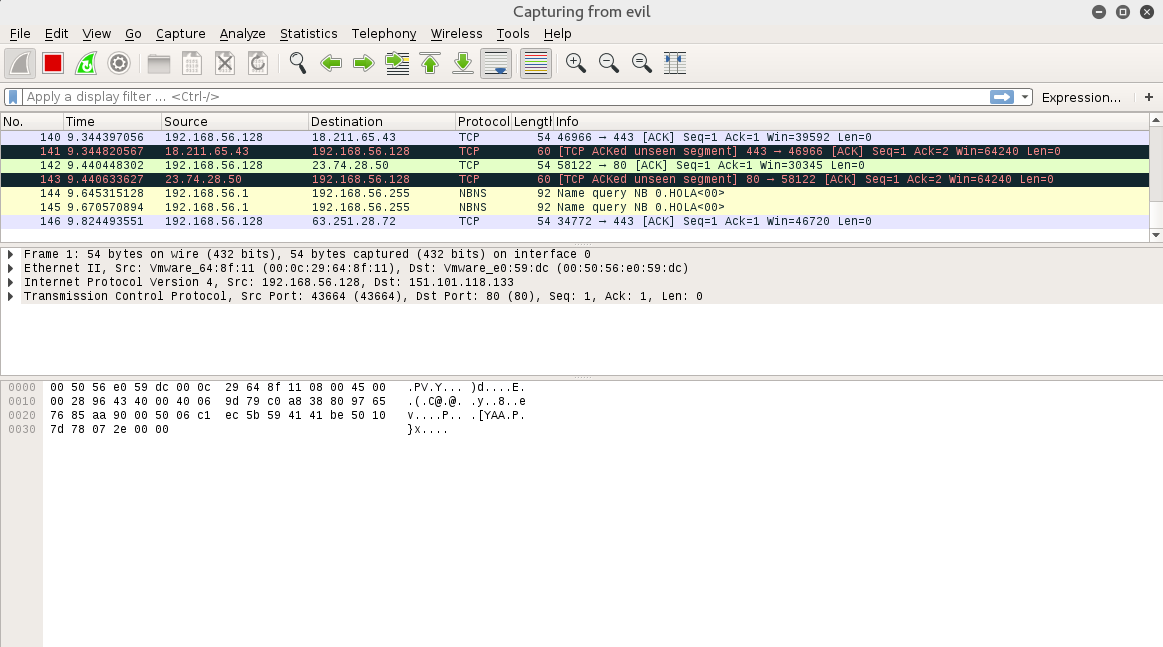
**Appendix A: Wifi network 'GiantHavok' details**

****

**Appendix B: Communications interference**

****

**Appendix B: Man in the Middle network traffic**

****

**Appendix B: Man in the Middle network traffic**