**Mobile Infrastructure Security Assessment Report**

**Conducted by Brendan Murphy**

**2/26/2019**

Contents

[1. Executive Summary 3](#_Toc460650571)

[2. Test Parameters 3](#_Toc460650572)

[3. Targets 3](#_Toc460650573)

[4. Analysis 4](#_Toc460650574)

[5. Appendix A 7](#_Toc460650575)

[6. Appendix B 7](#_Toc460650576)

[7. Appendix C 7](#_Toc460650577)

# Executive Summary

The purpose of this document is to assess potential vulnerabilities of Wireless Access Points within a Small Office Home Office (“SOHO”) Wireless LAN (“WLAN”) the results of Infrastructure servers which perform backend processing of mobile applications.

The primary Wireless Access Point in my home office is the network "ButterBeef" which is a 2.4 GHz wireless network broadcasting on channel 11. This network is secured with a WIFI Protected Access (WPA2-PSK) security password which is known by 2 users. Using manual analysis and passive reconnaissance techniques, I have determined that the network is secure. However, there are various security measures which could be implemented to strengthen the security of the network. Firstly, it is unclear if the cable router/modem combination box (supplied by Comcast) is using the most up to date firmware. A call to Comcast should ensure that the modem has the latest patches and upgrades, minimizing attack scenarios that target outdated and unpatched software. Using the NMAP (network mapping) scan tool I have discovered that the modem has many open ports, including port 443 which is currently receiving packets on an unfiltered basis. Sealing off this port would further reduce the likelihood of a hacker gaining access to the device. Lastly, the network is vulnerable to the 'evil twin' attack scenario where an access point could be created that would allow a hacker to intercept data on the network. To reduce the possibility of data loss in this scenario I recommend changing the network password frequently. I also recommend including various punctuation marks and other grammatical symbols in the password to increase complexity which would further reduce the likelihood of a brute force password hack. A strong password is an excellent method to prevent against the creation of an evil twin network. Although the security of the network is intact, it is exposed to some serious hacking scenarios and security flaws that should be addresses as soon as possible to further secure the home network.

# Test Parameters

The Objective of this evaluation is to conduct automated testing of Server Side Controls. The Scope of this evaluation is **wlan0. wlan0** is a wireless network operating on 802.11. This Analysis includes Passive Reconnaissance analysis techniques and manual analysis techniques. Network Analysis tools include the following:

* **Kismet**
* **NMAP**
* **AirCrack**

# Targets

The Scope of the evaluation is as follows:

**Information Gathering**

* 1. wlan0

# Analysis

Table : Information Gathering

|  |  |  |
| --- | --- | --- |
| **INFRASTRUCTURE COMPONENT** | **DESCRIPTION** | **EVIDENCE** |
| **WiFi Network Channel\*** | **11** | **Appendix A** |
| **WiFi Network SSIDs\*** | **ButterBeef** | **Appendix A** |
| **External Network SSIDs\*** | **ButterBeef** | **Appendix A** |
| **Access Point BSSID\*** | **5C:E3:0E:CE:64:DC** | **Appendix A** |
| **Access Point Manufacturer\*** | **Unknown** | **Appendix A** |
| **Access Point Frequencies\*** | **2447, 2452, 2457, 2462, 2467** | **Appendix A** |
| **Access Point Type of Traffic\*** | **Beacon (advertising AP)** | **Appendix A** |
| **Access Point Seen by Interface\*** | **Managed/Infrastructure** | **Appendix A** |
| **WiFi Network # of Clients\*** | **4** | **Appendix A** |
| **WiFi Network Client List\*** | **Attached** | **Appendix A** |

**\*Kismet Analysis**

Table : Baseline Configuration Analysis

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **VULNERABILITY** | **YES** | **NO** | **DESCRIPTION** | **RISK LEVEL** | **EVIDENCE** | **RECOMMENDATION** |
| **Outdated Firmware Implemented\*** | **YES** | **NO** | **Website shows no drivers or firmware currently available** | **High** | **Appendix B** | **Contact Comcast about firmware update** |
| **Factory ESSID in Use\*\*** |  | **NO** | **Reset** | **Low** | **Appendix B** |  |
| **Default Administrative Username/Password in Use\*\*** |  | **NO** | **Reset just now** | **Low** | **Appendix B** |  |
| **Weak Administrative Password\*\*** |  | **NO** | **Reset just now** | **Low** | **Appendix B** |  |
| **Weak Authentication Protocols Supported\*\*** | **YES** |  | **Nmap showing many open protocols** | **Medium** | **Appendix B** | **Further research, reduce authentication protocols** |
| **Unnecessary Ports Open\*** | **YES** |  | **Nmap showing many open ports** | **Medium** | **Appendix B** | **Further research, close unnecessary ports** |
| **Open Ports Vulnerable to Known Exploits\*** | **YES** |  | **Nmap showing many open ports such as 443** | **Medium** | **Appendix B** | **Add a filter to port 443** |
| **Unencrypted Administrative Interface Available\*\*** | **YES** |  | **e.g. non-HTTPS access to 192.168.2.1 is accessible** | **High** | **Appendix B** | **Further Research, find a way to close** |
| **Security Alerts (syslog, trapes, etc.) are Not Enabled\*\*** |  | **NO** | **Unclear** | **Medium** | **Appendix B** | **Security Alerts are enabled** |
| **Filters are not in place to prevent against Unauthorized Protocols\*\*** |  | **NO** | **e.g. ARP, RIP, SNMP, NetBIOS, etc.)\*\*** | **Low** | **Appendix B** | **Comcast has standard blocked ports** |
| **Filters are not in place to prevent against user-to-user wireless\*\*** | **YES** |  | **Filter in places with medium security firewall** | **Medium** | **Appendix B** | **No recommendation at this time** |

**\*NMAP Analysis of AP**

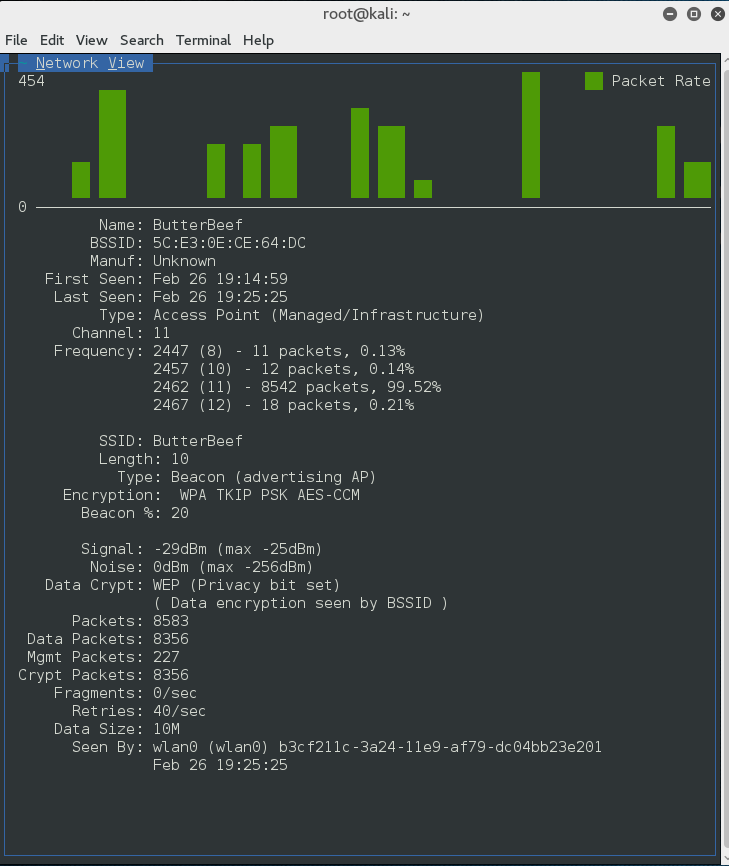
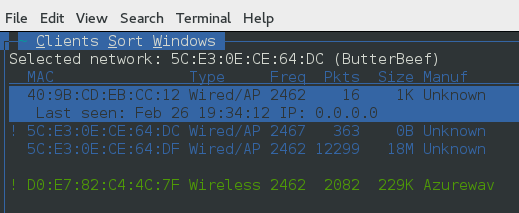
**\*\*Manual Analysis of AP Administrative Console Settings**

Table : Penetration Testing

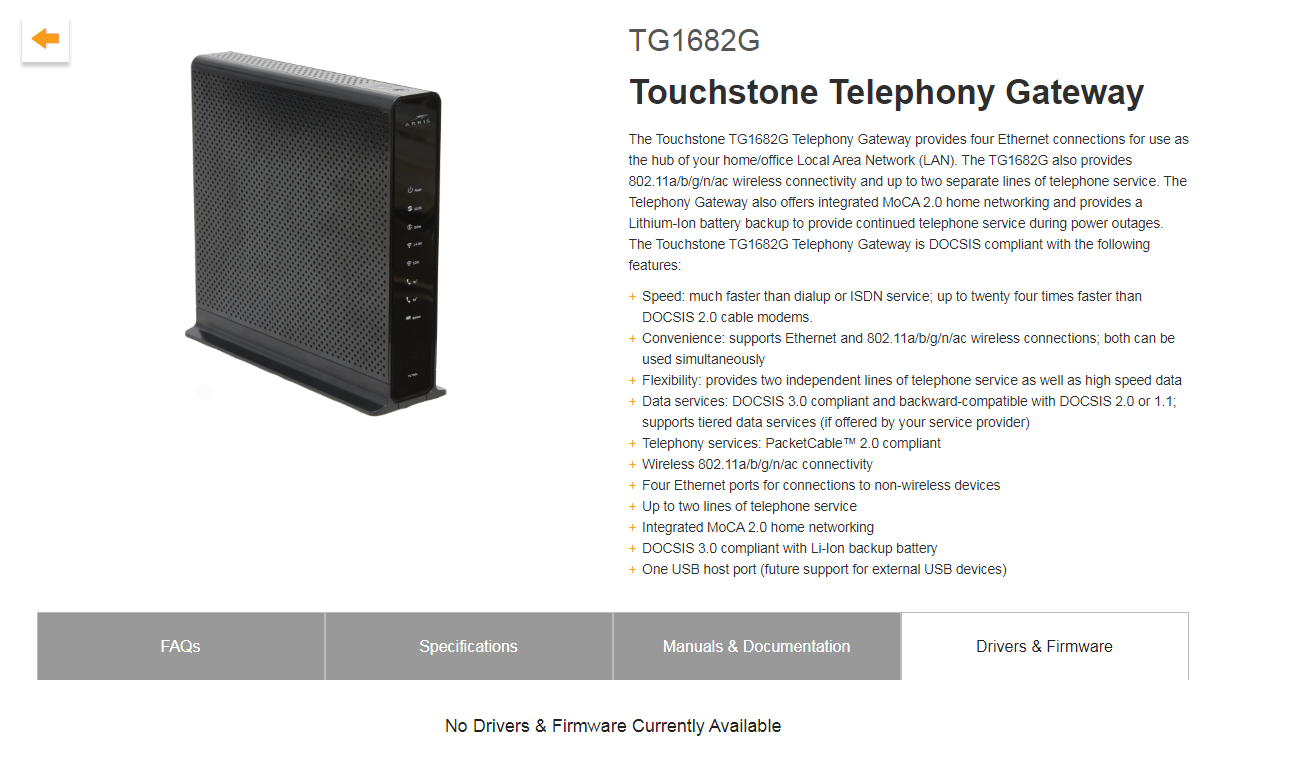
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **VULNERABILITY** | **YES** | **NO** | **DESCRIPTION** | **RISK LEVEL** | **EVIDENCE** | **RECOMMENDATION** |
| **Wireless Network Allows Rogue Access Points\*** | **YES** |  | **Was able to setup an evil twin access point** | **High** | **Appendix A – Section 3** | **Find a way to disable this feature** |
| **Wireless Network Clients Vulnerable to Mis-Association\*** |  | **NO** | **Was unable to access the evil twin network** | **LOW** | **Appendix A – Section 3** | **No Recommendation at this time** |

**\*AirCrack Penetration Testing**

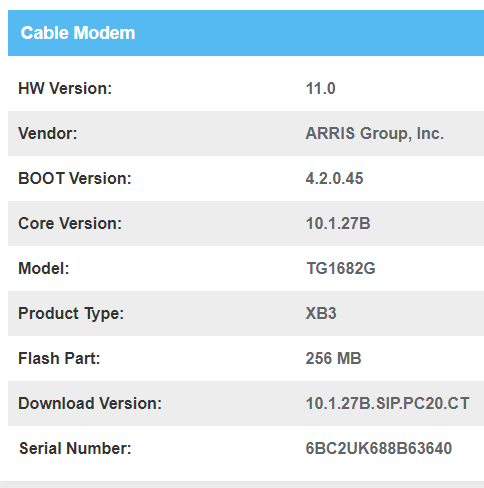
# Appendix A

** **

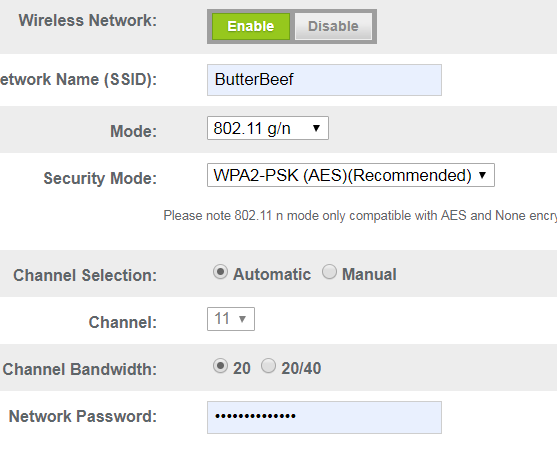
# Appendix B



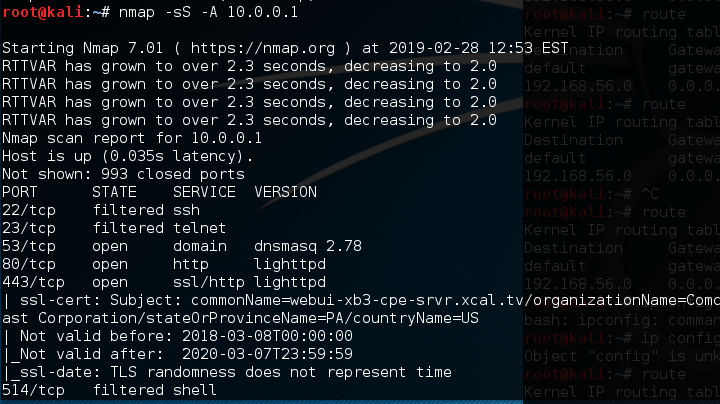
Firmware update unclear on TG1682G

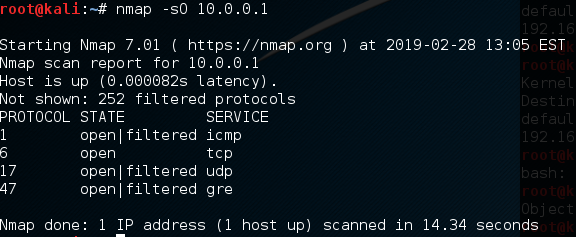


Firmware update unclear on TG1682G

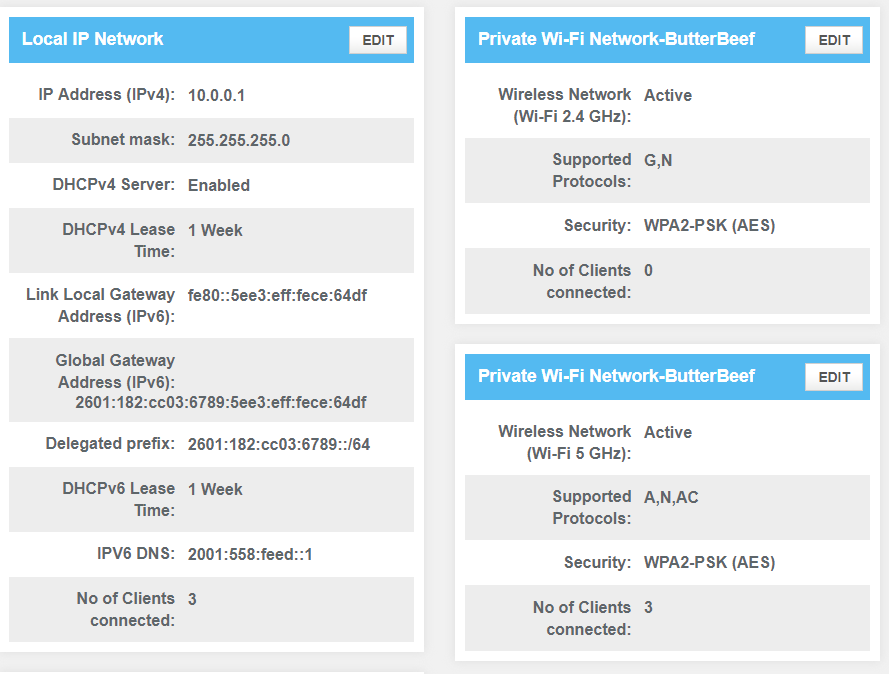


Reset factory WIFI/SSID

****

****

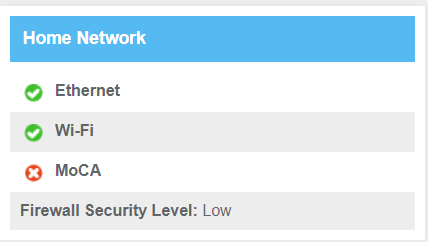
All open/filtered ports performed with nmap

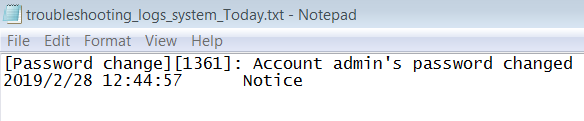
****

Unencrypted Administrative Interface Available

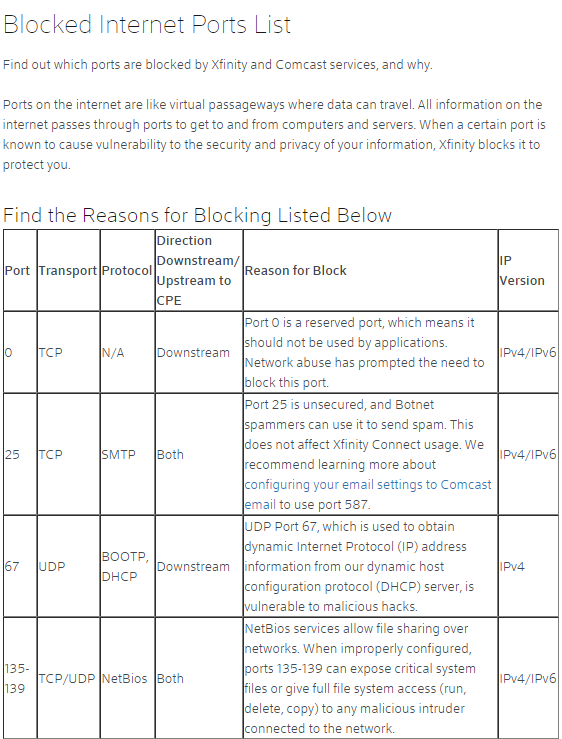
****

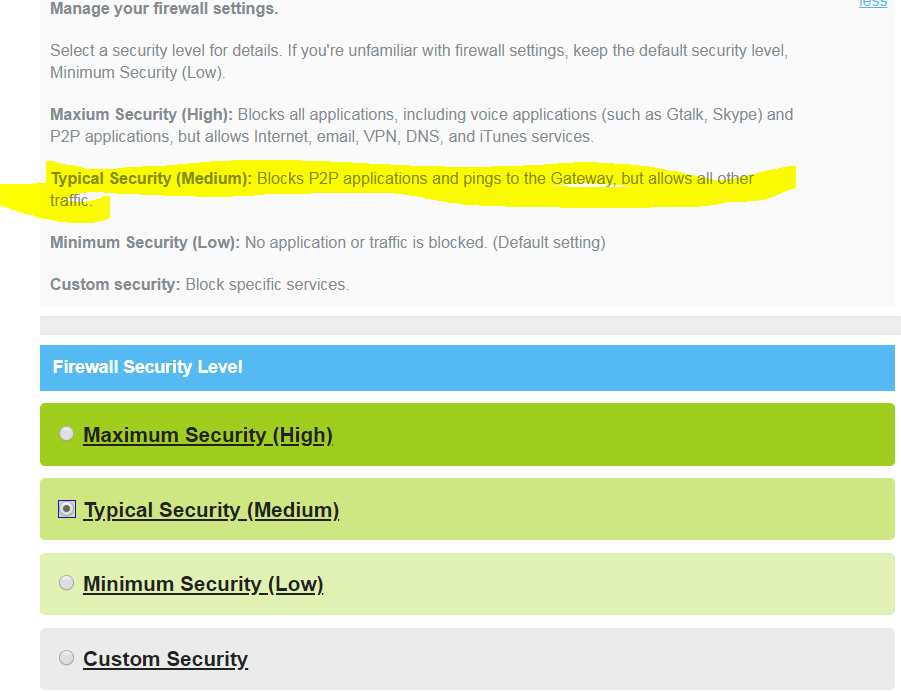
Firewall security level is low

****

****

**Security alert of password change appears in syslog**

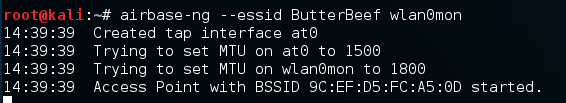
****

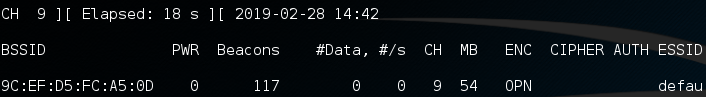
****

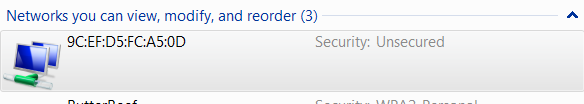
**Security to block Peer to peer applications**

# Appendix C

**(AirCrack Screenshots)**

****

****

****

**Could not connect to evil twin network**