

Wi-Fi Penetration Test

WPA WPA2

Masroor Khan S#1204399

BSc(Hons) Cloud Computing University of Wales Trinity St David, London, Email: 1204399@student.uwtsd.ac.uk

Introduction

- This was experimental based project.
- Different Wi-Fi protocol was explained
- Introduction to some famous attacks on Wi-Fi
- The discussion of tools which can help to prevent the attack



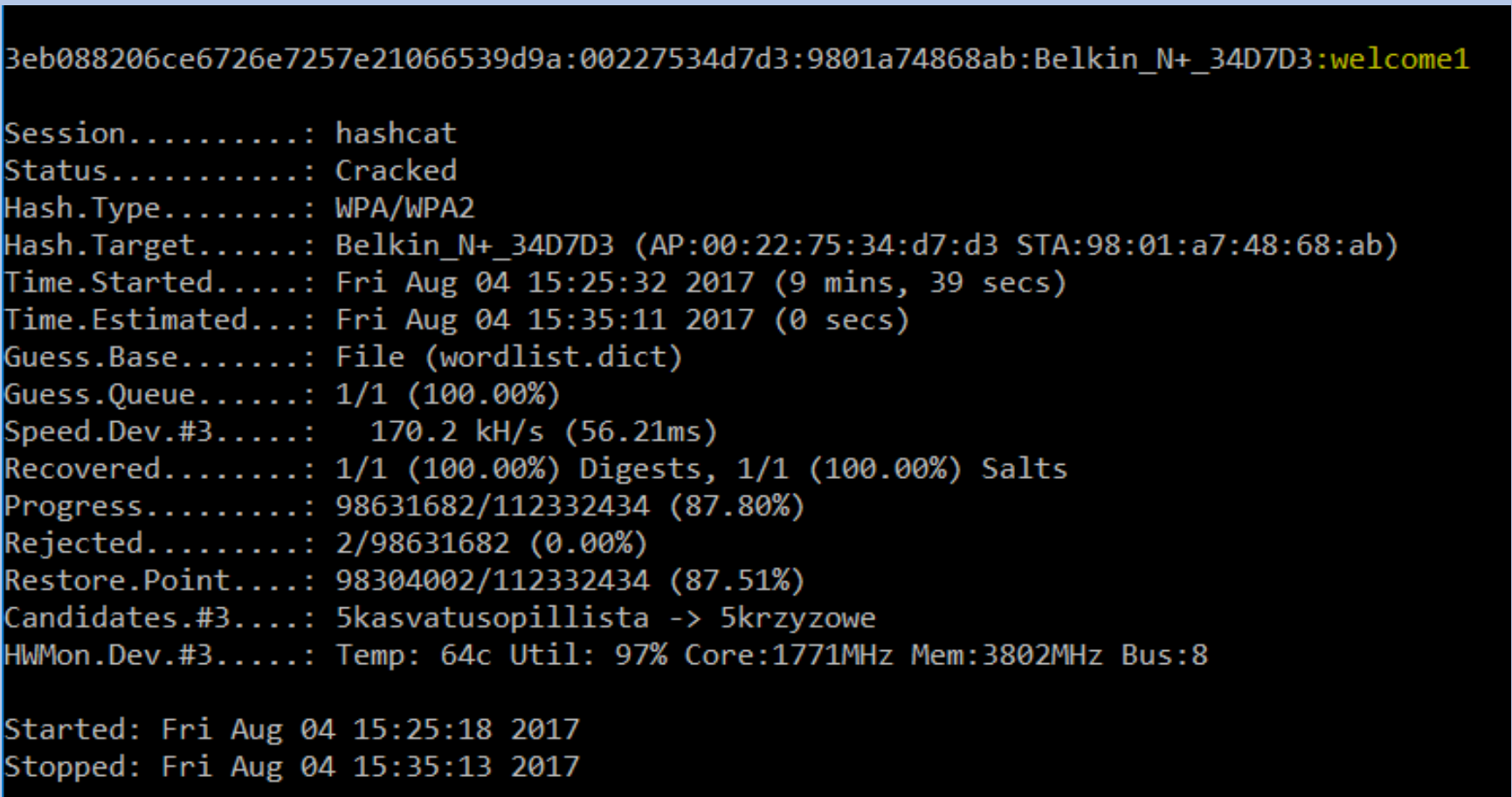
Aim & Goal

Test and measure Wi-Fi protocols and the critical evaluation of available security measures for implementation.

The goals are:

To test the Wi-Fi encryption techniques and identify relevant exposures. The attacks will try carry outs are:

- WPA/WPA2 key crack
- Brute force attack
- DoS (deauth packets)



HashCat Process

Motivation:

Wi-Fi network is quite easy to attack as compare to wired one, because can be access through air. Keeping Wi-Fi network secure is very important because future is wireless.

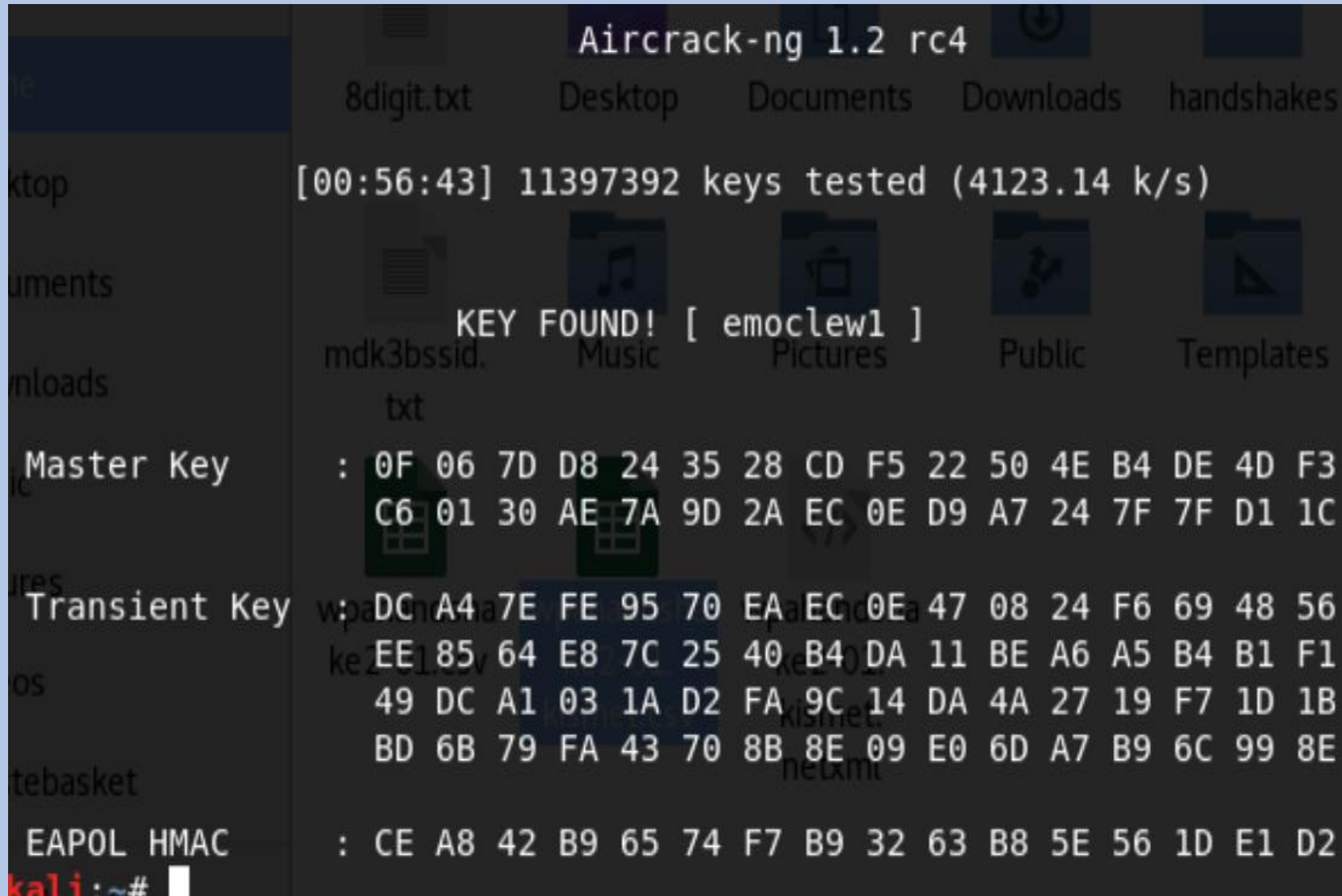


Practical work:

- WPS Key cracking through reaver was unsuccessful
- WPA successful in total 29 min through dictionary attack
- WPA non-dictionary attack using same alphabetic but scrambled successful in 60 mins

Purpose/ Completion

- WEP/WPA/WPA2 literature review
- Tested the WPA2 protocol,
 - WPS method was unsuccessful due to intelligent access point.
 - WPA2 handshake attack was successful
- The firewall exploitation time successfully recorded.
- Different key cracking tools was being used
- Set up the lab for practical work



Conclusion / Future Work:

- Showed the importance of better security method.
- Having complex passphrase for Wi-Fi near to impossible to crack.
- Limiting the range of Wi-Fi signals also an option to secure the network
- Using resources wisely with right tools increase the performance

- In future attacking the enterprise level network.
- Writing the better algorithm to overcome handshake capturing vulnerability

Wireless > Security

Security Mode >

WPA/WPA2-Personal (PSK) ▼

Authentication >

WPA-PSK ▼

Encryption Technique >

TKIP+AES ▼

Pre-shared Key (PSK) >

ecoclew1

