Experiment No:7

**Aim:** Password cracking using open source tool

**Theory:**

A password is the secret word or phrase that is used for the authentication process in various applications. It is used to gain access to accounts and resources. A password protects our accounts or resources from unauthorized access.

Password cracking is the process of guessing or recovering a password from stored locations or from data transmission system. It is used to get a password for unauthorized access or to recover a forgotten password. In penetration testing, it is used to check the security of an application.

In recent years, computer programmers have been trying to create algorithms for password cracking in less time. Most of the password cracking tools try to login with every possible combination of words. If login is successful, it means the password was found. If the password is strong enough with a combination of numbers, characters and special characters, this cracking method may take hours to weeks or months. A few password cracking tools use a dictionary that contains passwords. These tools are totally dependent on the dictionary, so success rate is lower.

Types of password cracking attacks:

Here’s I’ll be listing various types of password cracking attacks that are generally used by attackers:

* Dictionary attack: This attack uses a file that contains a list of words that are found in the dictionary. This mode matches different combinations of those words to crack your device open.
* Brute force attack: Apart from the dictionary words, brute force attack makes use of non-dictionary words too.
* Rainbow table attack: This attack comes along with pre-computed hashes. Thus, this method is faster.

**Aircrack-ng Suite:**

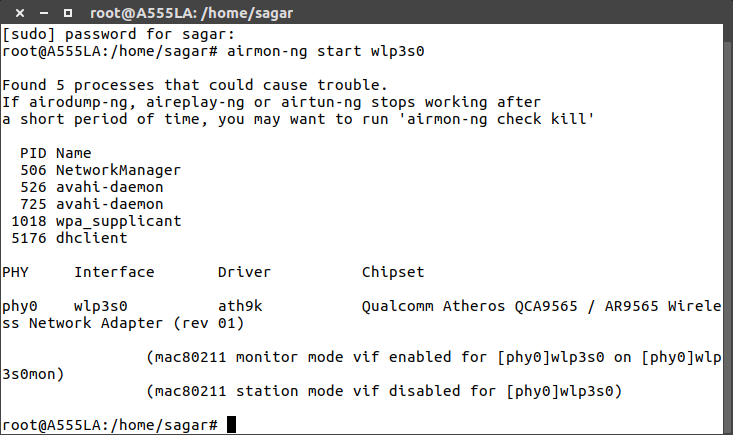
Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux, FreeBSD, OS X, OpenBSD, and Windows; the Linux version is packaged for OpenWrt and has also been ported to the Android, Zaurus PDA and Maemo platforms; and a proof of concept port has been made to the iPhone. Aircrack-ng is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

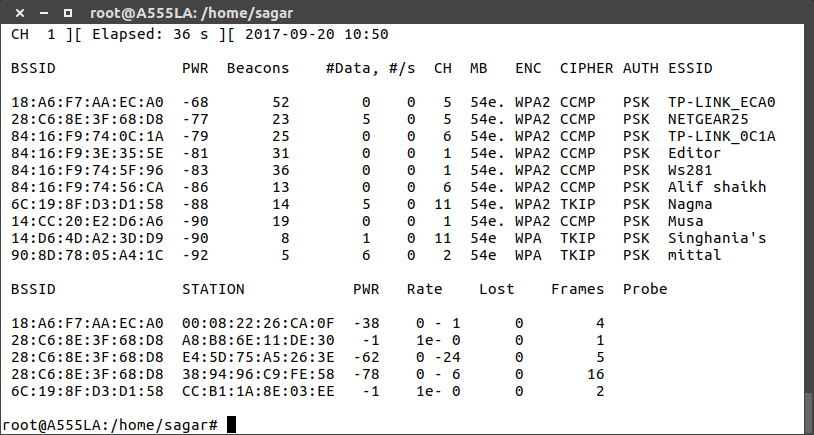
* Monitoring: Packet capture and export of data to text files for further processing by third party tools.
* Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.
* Testing: Checking WiFi cards and driver capabilities (capture and injection).
* Cracking: WEP and WPA PSK (WPA 1 and 2).

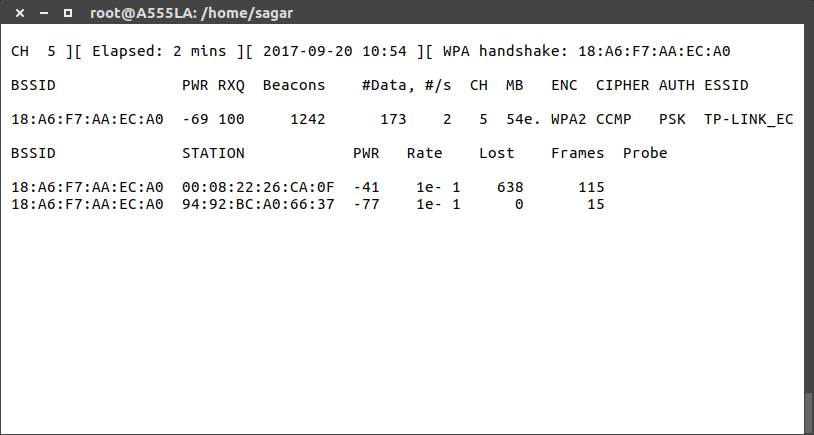
**Output:**

**Step 1: Start the wireless interface in monitor mode**

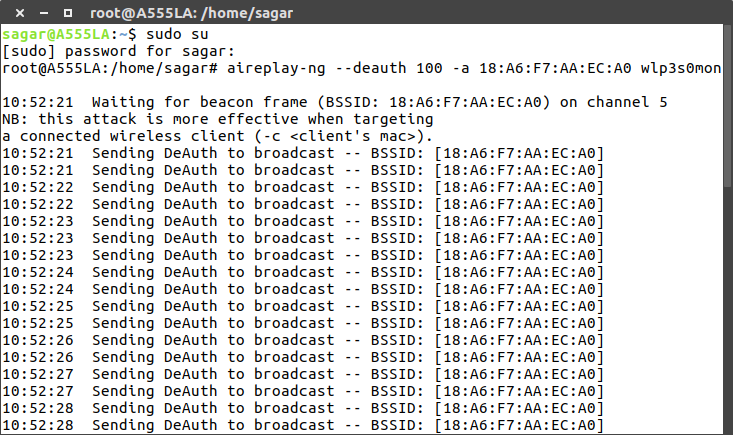


**Step 2: Start airodump-ng to collect authentication handshake**

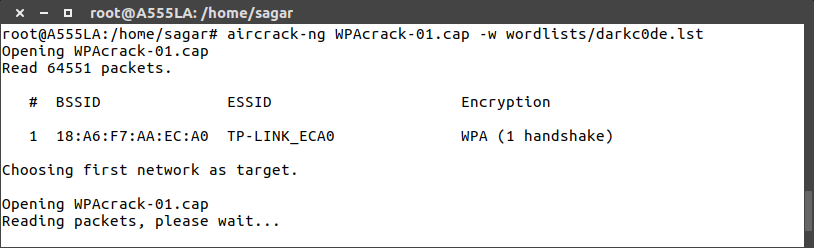
****

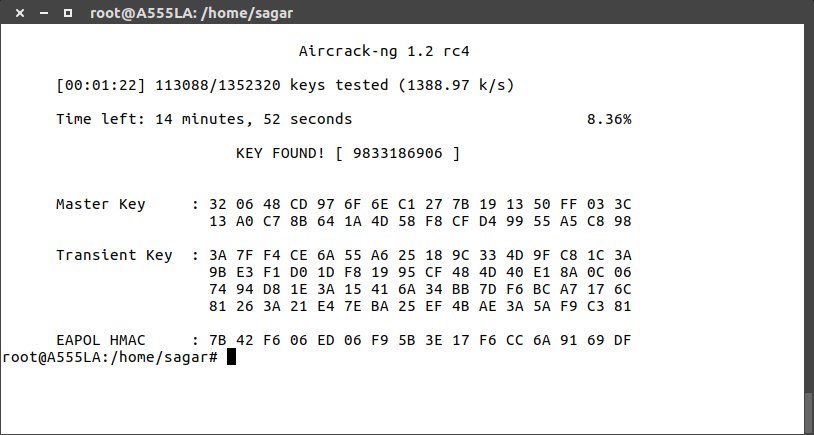
****

**Step 3** - **Use aireplay-ng to deauthenticate the wireless client**

****

**Step 4: Run aircrack-ng to crack the pre-shared key**

****

****

**Conclusion:**

Hence, the custom word file for all possible common passwords has been created and with the help of aircrack suite the working of password cracking has been demonstrated successfully.