Presenting A Novel Method For Wifi Password Recovery

Parvathi Vinod
Dept. of Computer Applications
Amal Jyothi College of Engineering
Koovappally, India
parvathivinod@mca.ajce.in

Vishnudev S
Dept. of Computer Applications
Amal Jyoyhi College of Engineering
Koovappally, India
vishnudevs@mca.ajce.in

Rincy Varghese
Dept. of Computer Applications
Amal Jyothi College of Engineering
Koovappally, India
rincyvarghese@mca.ajce.in

Sona Sebastian
Dept. of Computer Applications
Amal Jyothi College of Engineering
Koovappally, India
sonasebastian@amaljyothi.ac.in

***Abstract*—Password Cracking is the process of recovering passwords from data that have been stored in or transmitted through networks. One of the best wireless password hacking tools is Aircrack-ng for WEP/WAP/WPA2 cracking. The Aircrack-ng suite contains tools such as Aireplay-ng (to generate traffic and client de-authentication), Airodump-ng (packet capturing), and Airbase-ng (to configure fake access points). This combination of tools requires more interaction and time to get the capture file. In this paper, we use the Wifite tool to create the wpa.cap file. Wifite is a penetration tool that detects and lists out all the nearby Wi-Fi devices in a range. Wifite selects the target capture file, enables the de-authentication attack and does the handshake process. Cracking the password by matching wordlists and the capture file.**

Keywords—Aircrack-ng,DE-authentication,Handshaking Password Cracking , WEP/WAP2

I. INTRODUCTION

Wireless networks are commonly used all over the world. It is accessible to anyone within the router's transmission radius. This creates vulnerability and leads to password cracking. Password cracking is the process of finding the password by using a wordlist using a computer algorithm. The time taken for cracking the password will depend on the strength of the password. This paper examines how easily it can take up the capture file, which contains the raw data of wireless networks, and crack the password. By using the Wifite tool, we get the capture file. The crunch tool is used to generate wordlists (password) according to the user's guess. Finally, combining Aircrack-ng and Crunch password will be obtained.

II. RELATED WORKS

Sanja Maravić Čisar [1], Petar Čisar [1] have discussed the ethical hacking tools to check the vulnerabilities and securities of a Wi-Fi network. The key is found by cracking the password through different procedures using Linux tools. Chintan Kamani[2], Dhrumil Bhojani[2],Ravi Bhagyoday[2], Vivek Parmar[2], Deepti Dave[2] de-authentication is the transfer of target data between router and device.IEEE 802.11 protocol that is used in the de-authentication process.The de-authentication frame is from a router to disconnect the device forcefully. Tien-Ho Chang[3], Jiunn-Wu Lin[3], Chia-Mei Chen[3], Gu-Hsin Lai[3] there is a four-way handshaking technique to get the encrypted packet as the first step of password cracking. IDM(Intelligent Deauthentication Method) is proposed for easy access to capture file.Raghu Ram[4], D Sindhura[4], Maintaining the Integrity of the Specifications Osman Shareef[4] physical access or connection is not necessary to crack the password in wireless networks. The time taken to crack the password can determine the strength of the password. Martin Beck[5], Erik Tews[5] the key recovery attack of WEP can be minimized by reducing the average number of packets then the attacker has to intercept for the secret key. The pre-shared key is the most common dictionary attack of WAP.

III. INTRODUCTION TO TOOLS

A. Aircrack-ng

Aircrack-ng is a penetration testing tool that is used to crack WEP and WAP2 keys. The purpose of Aircrack-ng is to recover WiFi passwords using the capture file and cross-check with a wordlist. Aircrack-ng can recover keys once enough data packets have been captured.

B. Wifite

Wifite is a penetration that detects and lists out all the nearby Wi-Fi devices in a range. It is used to create the wpa.cap file. Wifite selects the target capture file, enables the de-authentication attack and does the handshake process.

C. Crunch

Crunch is a wordlist generator that can generate all possible combinations and permutations. Crunch is used to generating wordlists according to the user's guess.

IV. WORKING

The wifite tool finds out all nearby Wi-Fi devices and we can lock target device. By locking a target device, the DE authentication packets are sent until handshake process have been done. As a result, its capture file will be stored in the system. The capture file contains raw data of target device like encrypted password, name etc. Finally, by integrating crunch and aircrack-ng it's possible to find out the password. Crunch will be generating random passwords according to the user needs such as maximum and minimum length, characters to be checked and patterns. Aircrack-ng matches wordlist and capture file for the result. Whenever a key is found the process will be stopped and the result will be displayed.

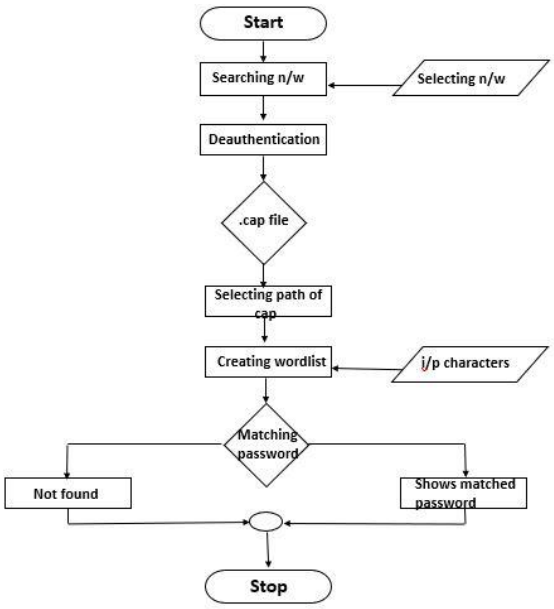

Figure 1:Working of tools

V. IMPLEMENTATION AND RESULTS

Demonstration of Wi-Fi password recovery using Aircrack-ng, Wifite and Crunch.

A. List of Wi-Fi devices

First up all we need to find out nearby devices which provides internet. By the use of wifite tool we can list near by devices. It shows number, ESSID, Channel number, Strength of the connection etc.

Wifite

Wifite is a single command which list all the nearby devices.

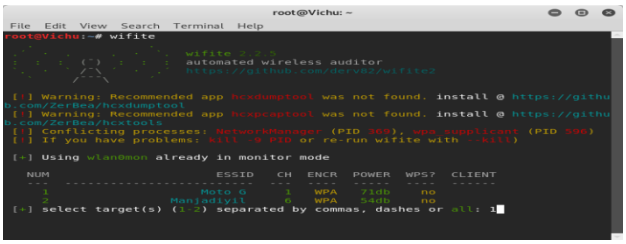

Figure 2: Scanning a network

B. Target a device

Lock any of the device which should be recovered. By locking a target device, the de-authentication packets are sent until handshake process have been done. As a result, its capture file will be stored in the system. The capture file contains raw data of target device like encrypted password, name etc. Selecting target device by entering order number.

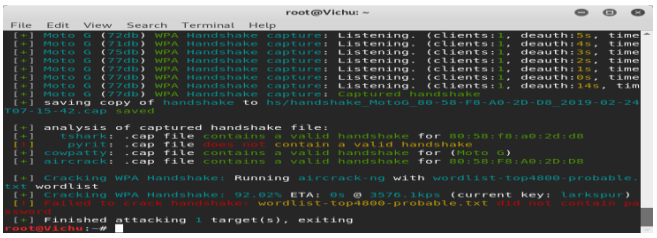

Figure3: Deauthentication and handshake process.

C. Integration of crunch and aircrack-ng

Finally, by integrating crunch and aircrack-ng its possible to find out the password. Crunch will be generating random passwords according to the user needs such as maximum and minimum length, characters to be checked and patterns.

crunch 8 8 –t 0000%%%% 0123456789 | aircrack-ng –w - /root/hs/*.cap –e Moto G

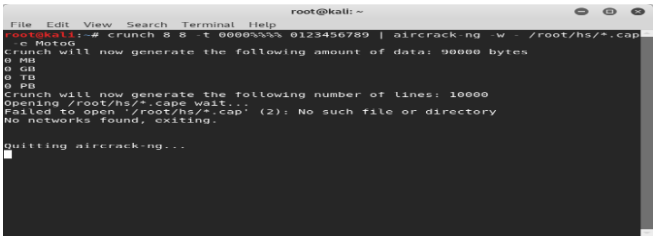

Figure4: Crunch and aircrack-ng

D. Recovering Password

Aircrack-ng matches wordlist and capture file for the result. The wordlist dynamically creating using crunch tool and we should select the path. ESSID have to be given in aircrack-ng tool to identify the device. Whenever a key is found the process will be stopped and the result will be displayed.

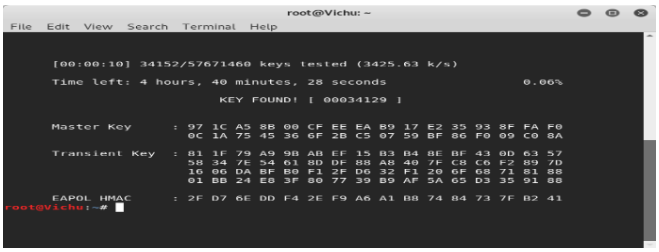

Figure 5: Recovery

VI. CONCLUSIONS

The purpose of Aircrack-ng is to recover Wi-Fi passwords using the capture file and cross-check with a wordlist. Now we use the Wifite and crunch tool in combination with the Aircrack-ng which makes the handshaking process easy and which helps in getting capture

file quickly. The crunch tool generates wordlist according to the user's preference.

REFERENCES

[1] Petar CISAR,Sanja Maravic CISAR, “Ethical Hacking Of Wireless Networks In Kali Linux Environment,” . Academy of Criminalistic and Police Studies,1.11080 Belgrade-Zemun, Cara Dusana 196,SERBIA 2.Subotica Tech,24000 Subotica, Marka Oreskovica 16, SERBIA.

[2] Chintan Kamani, Dhrumil Bhojani, Ravi Bhagyoday, Vivek Parmar, Deepti Dave, ”De-Authentication Attack on Wireless Network,” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-3S, February 2019.11111

[3] Manual-Tien-Ho Chang,Jiunn-Wu Lin,Chia-Mei Chen,Gu-Hsin Lai, ”The Method of Capturing the Encrypted Password Packets of WPA & WPA2,” Automatic, Semi-Automatic or Manual

[4] Aaron L.- F. Han, Derek F. Wong, Lidia S. Chao, “Advances of Password Cracking and Countermeasures in Computer Security,” *NLP2CT Lab, University of Macau, Macau SAR ^ILLC, University of Amsterdam, Science Park 107, 1098 XG Amsterdam.

[5] Sheikh Md. Rabiul Islam, “Wi-Fi Protected Access (WPA) –PSK (Phase Shift Keying) Key Cracking Using AIRCRACK-NG,” International Journal of Scientific & Engineering Research ,Volume 4, Issue 9, September -2013 2021 ISSN 2229-5518