Academic Journal of Nawroz University (AJNU), Vol.10, No.1, 2021

https://doi.org/10.25007/ajnu.v10n1a998

Penetration Testing: Wireless Network Attacks Methods on Kali Linux OS

Renas R. Asaad,
Department of Computer Science & I.T, Nawroz University, Duhok, Kurdistan Region – Iraq

ABSTRACT

This paper implements a wireless attack technique by cracking the password on kali Linux OS using Hashcat technique. This study identifies the security weakness, using brute-force attack for online attacking and straight attack for offline attacking. The brute-force attack is also recognized as a detailed search, where it attempts guessing the target password one password at a time until reaching the correct password, which is called a dictionary attack. then using hash algorithms to deal with MD5 hash algorithm and SHA-512 (Linux). In this article, we will learn about the various wireless attacks. These days, wireless networks are everywhere. With users being on the go like never before, having to remain stationary because of having to plug into an Ethernet cable to gain Internet access is not feasible. For this convenience, wireless connections are not as secure as Ethernet connections. In this article, we will explore various methods for manipulating wireless attacks and their techniques including several methods on Linux.

Keywords: Wireless Network, Hashcat, Vulnerability Assessment, Kali Linux.

1. Introduction

Wireless networks become useful nowadays. They utilized all over the world in several fields of security, at domestic, at work and indeed open places in arrange to associate to the Web and do a trade or private things [1,2]. Other than all the points of interest in making commerce and life simpler, there are certain downsides in terms of dangers. The frailty of remote systems has been causing a part of inconvenience in terms of breaking into banks, companies, and government organizations. The recurrence of these assaults is as it heightened, as to organize chairmen are not completely harmonized when it comes to securing remote systems in a strong and reliable way[3]. A remote network can be split utilizing Kali Linux working framework and it'll be spoken to within the segment that takes after. Remote systems have gotten to display all over. They are used all over the world totally different regions of life, at domestic, at work and indeed open places in arrange to associate to the Web and do commerce or private things[1,4].

2. Literature Review

Kali Linux is the world's most powerful and popular penetration testing platform, used by security professionals in a wide range of specializations, including penetration testing, forensics, reverse engineering, and vulnerability assessment. It is the culmination of years of refinement and the result of a continuous evolution of the platform, from WHoppiX to WHAX, to BackTrack, and now to a complete penetration testing framework leveraging many features of Debian GNU/Linux and the vibrant open source community worldwide. Kali Linux has not been built to be a simple collection of tools, but rather a flexible framework that professional penetration testers, security enthusiasts, students, and amateurs can customize to fit their specific needs.

3. Implementation

A multifunctional device for wireless internet access „Huawei HG530“ by „Huawei Technologies“ will be

used for this cybersecurity research. As an end device a smart phone with operating system Android v4.2.2 is used. The attacking system is mobile computer with OS KALI LINUX, figure 1 shows explanation steps[2,5].

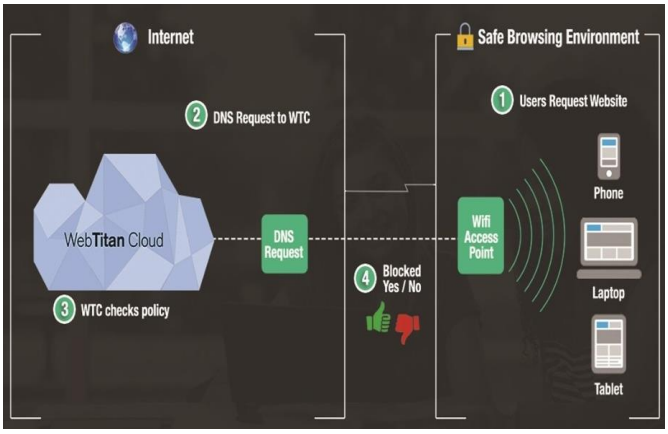


Fig. 1: Local Network

The KALI operating system uses a wide variety of network penetration test instruments, including "Aircrack", which are updated regularly. The free distribution helps all age audience with different technical skills to experience networks and systems security testing. The common well-known attack for the wireless networks is "Man-in-the-Middle" (MITM)[6]. Intrusions in social networks infrastructures are prohibited, and for this reason, a separate wireless network is built for the research purpose. The limited resources, like processing time and RAM memory in the test machine lead to possible variations in the results obtained with different equipment [7]. In this research, two test destinations will be used:

- network access by WPA-2 passphrase cracking.
- network access by WPS PIN exposure.

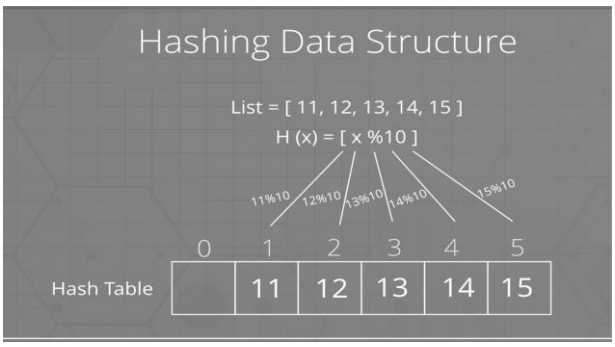


Fig.2: Hash Structure

3.1 Cracking Wireless Network in Kali Linux

In this section will discussed the two methods of cracking, and the two methods rely on different techniques to crack or break the safety barrier on victim's router, the methods are:

a. Online Method Depends on:
- Identify username.
- Check cat command for wordlist.
- Using Secure Shell Protocol.
- Brute-Force Attacking.

b. Offline Method Depends on:
- Message-Digest hashing (MD5).
- Hashcat algorithm.
- Hash Type "Sha-512 (Linux)".
- Straight attacking.
- Hash Type NTLM.

3.2 Packet Transfer:

Each manufactory generate a unique Media Access Control (MAC Address) to Identify PCs and its called a physical address[11,10]. For transferring any packet the MAC address and destination MAC are used. And it can be changed by "MAC Changer":

$$> ifconfig\ [type]\ down$$
$$> macchanger\ -m\ [MAC]\ [type]$$
$$> ifconfig\ [type]\ up$$

4. Common Methods of Attacks

4.1 Aircrack

Aircrack-ng, is a good point of contact together, and together, it represents the aggregation of networks, and the tool makes it possible to achieve this by means of grouping methods, guesswork platform, and great encryption of passwords, and grouping them together. Very good, very good on this page.

4.2 Wireshark

Wireshark tool, a tool designed in 1998 and created by the creator Gerald Combs, as for the language used was C and C ++, its main name was Ethereal, but it was changed in 2006 due to problems in choosing the brand, it is considered one of the tools of internal penetration, and we mean internal penetration Hacking local networks, the main goal of the tool is to listen and eavesdrop on the data that is passed on the

network, if I use Wireshark while I am connected to a Wifi network, I can spy on all the sites and files and everything that is circulating within that network, it is true that everything will pass It is encrypted before your eyes, but you can later decrypt it. The tool is also available in several systems.

4.3 OCLHashcat

OclHashcat uses what is called a brute force attack, and this tool is not included in the Alkali Linux system, but you can download it and add it to the rest of the tools, and it is considered one of the fastest tools to penetrate Wi-Fi networks.

4.4 Kali Net Hunter

It is based on the Kali Linux system, ROM. In short, the Kali Linux application is a ROM

And the process of installing it is carried out in specific types of phones, such as:

- Nexus
- OnePlus One

And some of the Samsung releases, and unofficially it can be installed on some other phones, the ultimate goal of the application remains to test the extent of Wi-Fi penetration through the tools provided by the Kali Linux application. In view of the advantages that this application provides to its users, it is one of the most famous competitors in the field of Wi-Fi penetration in the world, which makes it the ideal program to hack on Android. And the fame that we talk about through the responses of Kali Linux NetHunter shows the good reputation of the application of affirmative actions represented in the comments.

Bellow the steps attacking a network through the specific victim router's, and shows the way to see the vulnerability in WPA, WPA-2. [9,10].

```
$ sudo apt-get install aircrack-ng
Turning airmong ON
                $ airmon − ng
Monitoring the Network
            $ airmon − ng start wlan0
Enabling MMI
                $ iwconfig
Stop and killing process that return errors
            $ airmon − ng check kill

Get all Routers
            $ airodump − ng mon0
After choosing a router name and checking
WPA/WPA-2 security, Then select and monitor it.
    $ airodump
    − ng  − c channel  − −bssid MAC  − w /root
    /Desktop/ mon0
Renaming the cap file
            $ mv ./−01. cap name. cap
Converting it to hccapx
    $ cap2hccapx. bin name. cap name. hccapx
Installing naïve hash cat from web-site
            $ sudo git clone https://github.com
                        /brannondorsey/naive
                        − hashcat
            $ cd naive − hash − cat
            $ curl  − L  − o dicts/rockyou. txt
$ HASH_FILE = name. hccapx POT_FILE
                = name. pot HASH_TYPE
                = 2500 ./naive − hash − cat. sh
```

The cracked password is shown in the previous steps.

[cc lang="bash" width="780"]

```
$ aircrack − ng  − a2  − b MAC
                − w rockyou. txt name. cap
```

Figure 2 shows details and performance of hashcat method.

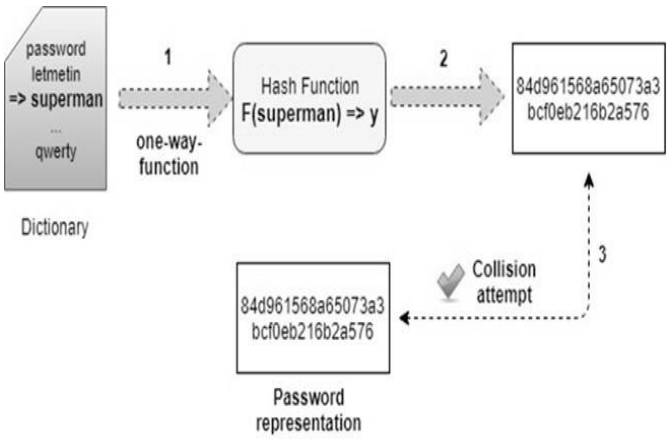


Fig.3: Hashcat Information Segmentation

4.5 SHA (512) Linux

The Secure Hash Algorithms (SHA) are a set of hash functions regularly utilized to hash passwords. By default, Curve employments SHA-512 for passwords, but a few frameworks may still be utilizing the MD5 algorithm. This article depicts how to extend password security[13], see figure 3.

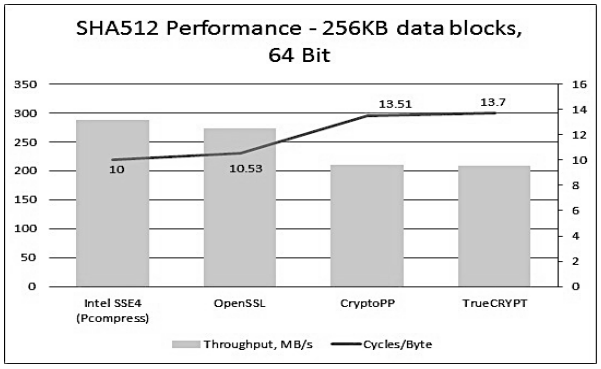


Fig.4: SHA-512 Performance

4.6 MD5 (Message-Digest) hashing:

When the user choosing or entering the password then this password will be hashed to be encrypted by MD5 hashing[(Asaad, 2020)]. For-example : password= 0001 will be encrypted to: **[EncryptedPass]**

Bellow figure 4 briefly steps of MD5 algorithm.

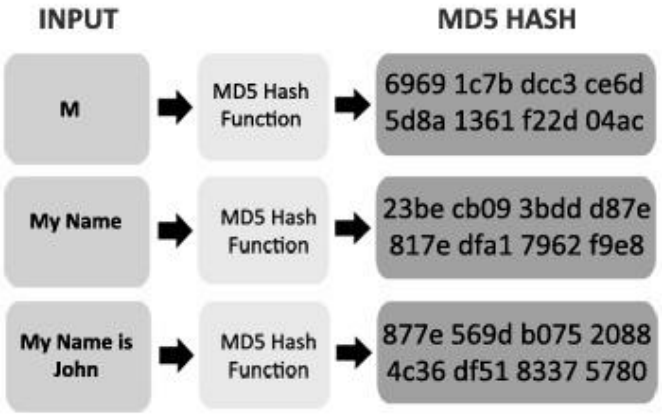


Fig.5: MD5 Hash Algorithm

5. Cryptography and Encryption Techniques and their Uses in Linux:

5.1 Encryption of Public Keys

Public-key cryptography uses a key (string) to encrypt and another to decrypt it, unlike other encryption methods that use the same key for the two tasks. The use of a private key for encryption (the public key) and another to decrypt it (the private key) aims to bypass the necessity to secure the transmission of the single key during the exchange of encrypted messages. Everyone's public key is available to everyone without exception, while the private key maintains a secret of its own. For example, when Muhammad wants to send encrypted mail to Omar, he uses Omar's public key to encrypt the mail. When the mail reaches Omar, he uses his private key, which no one else knows, to decrypt the message and view it. In this way, no one else will know the content of the message, Muhammad because he wrote the Unblinded Origin, and Umar is the only one who can decipher it.

5.2 PGP Program

PGP (short for Pretty Good Privacy) adopts the principle of encryption with public keys and can be used to sign and encrypt data: signing to verify the source and prevent impersonation, and encryption to maintain data privacy. Be aware, before using the program, of the legal restrictions in its use. In some countries, it is forbidden to send messages with a strong blindness outside the country.

5.3 TLS Protocol

TLS (and its earlier version SSL) is frequently used to secure communications in a computer network. The protocol aims to preserve the privacy of the data transmitted through communication by encrypting it, to authenticate the identities of communicators using public key cryptography, and to ensure the integrity of the data by collecting a checksum check for each data packet. The most popular Linux implementation of this standard is the OpenSSL library that supports cryptographic algorithms including DES, Blowfish, and IDEA.

5.4 HTTPS Protocol

It is an evolution of the HTTP protocol by including it within a TLS (or SSL) secured communication. The primary purposes of using HTTPS on websites are authentication, privacy protection and cross-data integrity verification.

5.5 S / MIME Protocol

The name is an acronym for the Secure Multipurpose Internet Mail Extension, which is an open standard that relies on public key cryptography to secure email and other types of communications on the network.

5.6 Virtual Private Network

There are several implementations of the secure IP standard on Linux. The IPSEC standard (acronym for Internet Protocol Security) is an effort behind the IETF Internet Engineering Task Force that aims to establish encrypted communications at the network level (Layer 3) and provide ways to verify data integrity, access control, authentication and confidentiality.

5.7 SSH Protocol

There are several software packages on Linux to use SSH, the most prominent of which is OpenSSH. SSH was designed to replace insecure remote communication protocols such as rlogin, rsh and rexec that were sending data with little security precautions. The OpenSSH software package relies on public key encryption to encrypt communications between host hosts and to authenticate users. It can also be used to log into a remote server or to copy data between hosts while protecting against man in the middle attacks and other attacks.

5.8 Pluggable Authentication Modules

Recent releases of Linux distributions come loaded with a unified authentication mechanism called Pluggable Authentication Modules, PAM that allows applications operating in user space to change their authentication requirements and method as needed. This mechanism can be used, among other things.

6. Attack Methods

In kali-linux has two ways to attack as shown in this section online and offline attack method

6.1 Attacking using Online Method:

$Kali - linux - pc : \sim\$\ cd/usr/share/wordlists$

$- \rightarrow Enter.$

$Kali - linux - pc :/usr/share/wordlists\$\ ls\ - \rightarrow Enter.$

dirb dnsmap.txt fern-wifi nmap.lst seclists dirbuster fasttrack.txt metasploit rockyou.txt.gz wfuzz

$Kali - linux - pc :/usr/share/wordlists\$\ sudo\ gzip$

$- d\ rockyou.txt.gz$

$[sudo]\ password\ for\ networkchuck:$

dirb dnsmap.txt fern-wifi nmap.lst seclists dirbuster fasttrack.txt metasploit rockyou.txt.gz wfuzz

$Kali - linux - pc :/usr/share$

$/wordlists\$\ cat\ rockyou.txt$

Will extract millions of suggested passwords", to reach it on advanced way so:

$Kali - linux - pc : \sim\$\ cat\ wordlist.txt$

$\$sudo\ hydra\ - L\ "username"\ - P\ wordlist.txt\ \backslash$

$>\ ["IP\ Address"]\ ssh$

SSH is a secure shell protocol and it's a safe way to login from one to another computer[(Asaad, 2020)].

[sudo] password for networkchuck: ["Victim's Network"]

["Password Generated"]

5.2 Attacking using Offline Method

$\$\ Sudo\ hashcat\ - a \rightarrow Enter$

$Kali - linux - pc: \sim\$\ man\ hashcat$

Attack Mode

0 = *Straight*

1 = *Combination*

3 = *Brute − force*

6 = *Hybrid Wordlist + Mask*

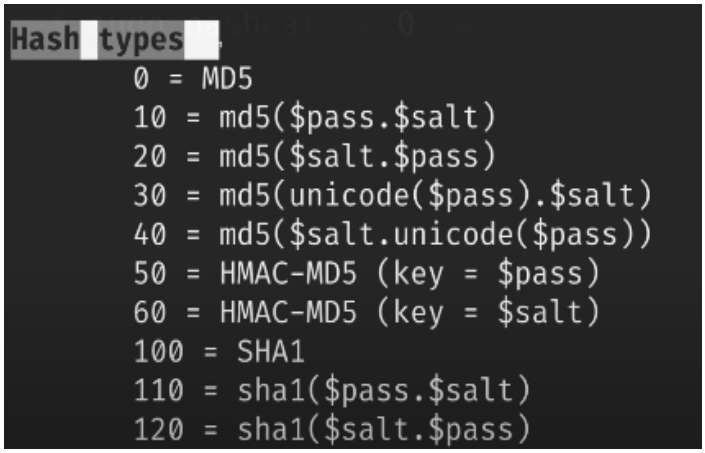
7 = *Hybrid Mask + Wordlist*

The attack is a straight mode for the next step.

$\$\ Sudo\ hashcat\ - a\ 0$

$- m \rightarrow Enter\ ["Hash\ types\ contain\ more\ than\ 7000\ types"]$

Then, when the Hash types appear we'll choose the (1800 = SHA-512 (Linux)) by writing it's number.



```
1720 = sha512($salt.$pass)
1730 = sha512(unicode($pass).$salt
1740 = sha512($salt.unicode($pass)
1750 = HMAC-SHA512 (key = $pass)
1760 = HMAC-SHA512 (key = $salt)
1800 = SHA-512(Unix)
2400 = Cisco-PIX MD5
2410 = Cisco-ASA MD5
2500 = WPA/WPA2
```

$ *Sudo hashcat* $-a\ 0\ -m\ 1800$
$-o\ crackedpasswords.txt\backslash$ → *Enter*
["1800 is a one the hashed types for SHA-512(Linux)"]
$>$ *hashes.txt wordlist.txt*
Thr:1 Vec:4
Recovered ...: ½ (50.00%) *Digests*,
Progress ... ...: 80/80 (100.00%)
Rejected ... ...: 0/80 (0.00%)
Restore.Point..: 40/40 (100.00%)
Restore.Sub.#1 ...: *Salt*: 1 *Amplifier*: 0 − 1 1
Candidates.#1 : *network* − *name* −> *extracted name*

Started: Date/Time
Stoped: Date/Time

$ Sudo hashcat -a 0 -m 1000 -o crackedpasswords.txt\
→Enter "1000 is a one of the hashed types for NTLM".
$>$ *"Hashed password here" wordlist.txt* →*Enter*
Session ……..: Hashcat
Status……..: Cracked
Hash.Name..: NTLM
Hash.Target..: [Physical Address]

$ *Sudo cat crackedpasswords.txt*
$ Sudo cat crackedpasswords.txt
[Physical Address]: [OriginalPassword]

6. Conclusion

Penetration testing helps to secure networks, and highlights the security issues. In this paper investigate different aspects of penetration testing including tools, attack methodologies and implementing some methods on Linux OS specific in Kali Linux, using some methods such as hashcat SHA-512 with their techniques. Then this implementation supports some unique modes of attack for over 200 highly-optimized hashing algorithms. And it's also support CPUs, GPUs, and some hardware accelerators on Linux, Windows, and OSX, and has facilities to help enable distributed password cracking. It's same when passing commands to Hashcat then automatically using the best method to crack passwords, either CPU or GPU depending on the Graphics driver you have installed or not. In this paper shows that the way to use a vulnerability to reset a password and benefit for this in an ethical hacking.

7. References

1. Bing, H. (2012, January). Analysis and research of system security based on android. In 2012 Fifth International Conference on Intelligent Computation Technology and Automation (pp. 581-584). IEEE.
2. Broad J, Bindner A, Hacking with Kali – Practical Penetration Testing Techniques, Elsevier, 2014., ISBN: 978-0-12-407749-2. Retrieved from: ftp://lab.dnict.vn/1.DNICT/2.Ebooks/books/Hacking%20with%20Kali.pdf.
3. Bradley M, (2017, June 9) An Overview of Wireless Protected Access 2. Retrieved from: https://www.lifewire.com/what-is-wpa2-818352
4. Step By Step Kali Linux and Wireless Hacking Basics-WEP Hacking (2015, May 19). Retrieved from: http://www.wirelesshack.org/step-by-step-kali-linux-and-wireless-hacking-basics-wep-hacking-part-3.html
5. Borges A (2014, February 20), Cracking Wireless Networks. Retrieved from: https://alexandreborgesbrazil.files.wordpress.com/2014/02/cracking_wep_networks1.pdf
6. d'Otreppe T, Introduction to WiFi Security and Aircrack-ng, Wireshark Developer and User Conference-Sharkfest 2012, UC Berkeley, June 24 – 27. 2012. Retrieved from: https://sharkfestus.wireshark.org/sharkfest.12/presentations/MB-Introduction_to_WiFi_Security_and_Aircrack-ng.pdf
7. Sabih Z, Learn Ethical Hacking From Scratch. Retrieved from: https://www.udemy.com/learn-ethical-hackingfrom-scratch/learn/v4/content.
8. Aircrack command series, URL: https://www.aircrack-ng.org/doku.php?id=aircrack-ng#wpa
9. WPS explained, URL: https://www.wi-fi.org/discover-wi-fi/wifi-protected-setup
10. Pixie Dust Attack explained, URL: https://forums.kali.org/showthread.php?24286-WPS-Pixie-DustAttack-(Offline-WPS-Attack)
11. Sak B., Ram J. Mastering Kali Linux Wireless Pentesting, Packt, 2016, ISBN 978-1-78528-556-1, p.p. 97-99, Available from: http://it-ebooks.info/book/1461060711/
12. Asaad, R. R. (2020). Implementation of a Virus with Treatment and Protection Methods. ICONTECH INTERNATIONAL JOURNAL, 4(2), 28-34.
13. Gueron, S., Johnson, S., & Walker, J. (2011, April). SHA-512/256. In 2011 Eighth International Conference on Information Technology: New Generations (pp. 354-358). IEEE.
14. Ramachandran V, Buchanan C, Kali Linux Wireless Penetration Testing Learn to Penetrate Wi-Fi and Wireless Networks to Secure your System from Vulnerabilities, 2nd Edition, Packt Publishing, 2015, ISBN-10: 1783280417