

# PENTEST BASED NETWORK SECURITY ASSESSMENT

P. Sindhu<sup>1</sup>, K. Naveen<sup>2</sup>, P. Akash<sup>3</sup>, K. Uday Bhaskar<sup>4</sup>, Bhargavi Kanuri<sup>5</sup>

<sup>1,2,3,4</sup> Student, Department of CSE, Gudlavalleru Engineering College, Andhra Pradesh

<sup>5</sup>(M.Tech), Assistant Professor, Department of CSE, Gudlavalleru Engineering College, Andhra Pradesh

**Abstract:** *In today's world security has been the utmost concern for any individual or an organization. With the evolving technologies and advances in computer security, threats and security attacks are increasing rapidly and will also increase in the future with the Internet of Things (IoT). Security is to give protection to the network or system. Everyone wants to keep their data safe and secure and in this new era of security, a voluminous amount of data is generated daily and the late detection of security threats can cause irreparable damage which becomes more worrisome. The fact is that more and more major security breaches are occurring where mainly the insecurity of wireless networks are causing a lot of trouble in terms of breaking into banks, companies, and government organizations. The frequency of these attacks is only intensified, as network administrators are not fully chimed when it comes to securing wireless networks robust and reliable way. This project is related to wireless network security problems. Kali Linux which is an Advanced Penetration Testing Linux distribution is used for Penetration Testing, Ethical Hacking, and network security assessments.*

**Keywords—** *Wireless networks, Wi-Fi Security, Penetration Testing, Ethical hacking, Network security*

## I. INTRODUCTION

Wireless networks are present everywhere. A wireless network allows devices to stay connected to the network but roam untethered to any wires. Access points amplify Wi-Fi signals, so a device can be far from a router but still be connected to the network. When we connect to a Wi-Fi hotspot at a cafe, a hotel, an airport lounge, or another public place, we are connecting to that business's wireless network or private matters. There are many advantages of using wireless networks in terms of, reduced cost, expandability, easy setup, productivity, mobility, convenience. Besides all the advantages of making business and life easier, there are certain drawbacks in terms of risks. The insecurity of wireless networks has been causing a lot of trouble in terms of breaking into banks, companies, and government organizations. The frequency of these attacks is only intensified, as network administrators are not fully harmonized when it comes to securing wireless networks robustly and reliably.

Penetration testing is a controlled simulated attack to identify the potential flaws and weaknesses within a business network, devices, or applications that can result in a data breach and financial loss. Penetration testing, also known as ethical hacking or pen testing, can focus on the business needs and wants but can include internal network security testing, external network security testing, web application testing. The purpose of penetration testing is to help the business and IT leadership identify vulnerabilities within their environment, leading to an attacker accessing privately-owned networks, systems, and sensitive business information. Once the vulnerabilities are discovered, penetration tester try to exploit these vulnerabilities to access information, elevate the privileges of a user's account, or take control of the business network. Penetration tests are conducted under strict rules mutually agreed upon by both the company in charge of performing the penetration test and requesting the assessment. Thus, Penetration testing verifies the ability of a system to protect its networks, applications, endpoints, and users against both internal and external threats. Also, it aims to secure the system controls and shuns any attempt of unauthorized access.

## II. RELATED WORK

In the previous years, pen testing has become an important area and several studies have developed and applied to improve more security in data, systems, and networks. However, there were a few mapping studies, surveys, or overviews that gather this information to show that what researchers have done and what all directions they should follow.

Mirjalili and Alidoosti[8] presented a survey about web pentest, discussed models, and compared the vulnerability scanning tools. Besides, they gathered works that have new proposals of the methods or tools for the web pentest. Their work shows a selection of primary studies that have been identified in three different ways: studies comparing the methods and tools that already exist, studies suggesting a new method or tool, and studies that suggest test environments for web pentest. Firstly, the research shows a comparison between 13 different open-source scanning tools, evaluating different criteria regarding their structure (interface, settings, usability, stability, and performance) and their features (spider, manual crawl, file analysis, logging, and reports). A comparison regarding the same criteria is also performed among the seven commercial scanning tools, by evaluating only their features. In general, the author's main contributions are around the relationship between the operation of the vulnerability scanning tools and its application scenarios, target environments, and limitations.

Al-Ghamdi[9] discussed the existing security testing techniques. The study focuses on the pentest considering all other test techniques, such as fuzz testing, binary code analysis, and vulnerability scanning. Conceptually, the author treats the pen testing as ethical hacking and highlights the division of the pentest into a black box, white box, and gray box.

Bishop[10] discussed the correct interpretation of the pentest by reiterating the need for detailed analysis about the activities that are been a part of pen testing. In the same way, Geer and Harthorne explained the main approaches and opinions about pen testing in a study that is used by several different studies as a conceptual base.

### III. METHODOLOGY

Hacking is typically legal as long as it is being done to search out the weaknesses in a computer or a network system for testing purposes. This sort of hacking is known as Ethical Hacking. There could be various positive and negative intentions behind the performance of hacking activities. Different security training manuals justify the process of ethical hacking in several ways, but for a certified Ethical Hacker, the entire process can be broken down into the following four phases.

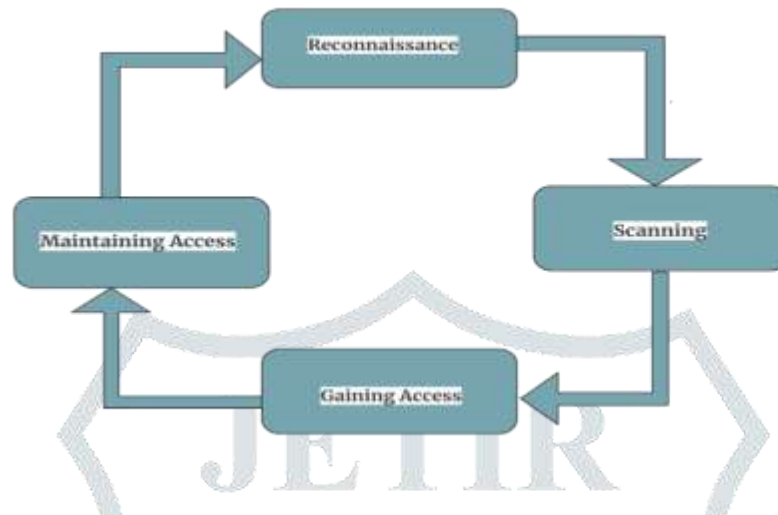


Fig 1: Phases of Ethical Hacking

#### A. Reconnaissance:

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. It may include identifying the target, finding out the target's IP address range, BSSIDs, network, DNS records, etc. In this project, we need the BSSID of the target network, so we follow this phase to get the information about the targeted Wi-Fi network.

#### B. Scanning:

In this phase, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Aircrack-ng. Using this tool the ethical hacker scans for vulnerability and captures the packets of a target network. This scanning of packets can be captured when we have a Kali Linux installed in our PC and a Wi-Fi adapter that follows monitoring mode and packet injection. The use of having monitor mode is to monitor all traffic received on a wireless channel and packet injection for interfering with an established network connection through constructing packets to appear as if they are part of the normal communication stream.

#### C. Gaining Access:

In this phase, we can design the blueprint of the network of the target with help of the information gained during the Reconnaissance and Scanning phase. Using the obtained data we now decide to gain access to a wireless network and this can be done by a De-authentication attack. These attacks allow us to disconnect any device from any network that is within our range even if the network has encryption or uses a key. This causes the client to reconnect the network where we can capture it by Four-way Handshake.

1) *Four-way Handshake*: In WPA-2 we get a four-way handshake process. It is designed so that access points and wireless clients can prove that they know each other by showing that they know the PSK/PMK, without ever releasing any of the keys. We must encrypt messages to each other, and if we can decrypt them, then they are successfully authenticated to each other. In this way, we can protect our network against a malicious spoof access point that is broadcasting the valid Id looking like SSID.

In the overall process, the PMK will last for the complete authentication of the devices and should be used sparingly. Thus four-way handshake uses derive key known as the Pairwise Transient Key (PTK), and which is generated from PMK, a client nonce, an access point nonce, and MAC addresses of the client and access point (AP). These are then put into a pseudo-random function, and then generate a GTK (Group Temporal Key). The GTK is then used to decrypt the multicast and broadcast traffic.

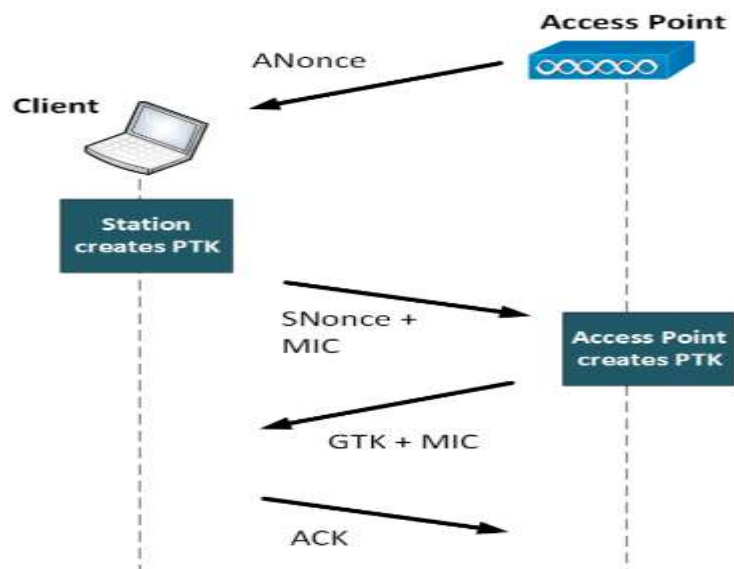


Fig 2: Four-way Handshake

The details of the handshake are as follows:

- AP sends a nonce to STA (ANonce). The client creates the PTK.
- Client nonce (SNonce) to AP and Message Integrity Code (MIC) which includes authentication.
- The AP creates PTK and sends GTK, along with a sequence number together and a MIC.
- The client sends a confirmation to AP.

#### D. Maintaining Access:

Once the ethical hacker gains the four-way handshake file from a target access point, now we can use air crack-ng to crack the key for the target AP. The air crack-ng will be going through the wordlist file, combine each password with the name of the target AP. If the network's password matches with wordlists password then we can completely crack the password of a target network.

## IV. RESULTS AND DISCUSSION

#### A. Results:

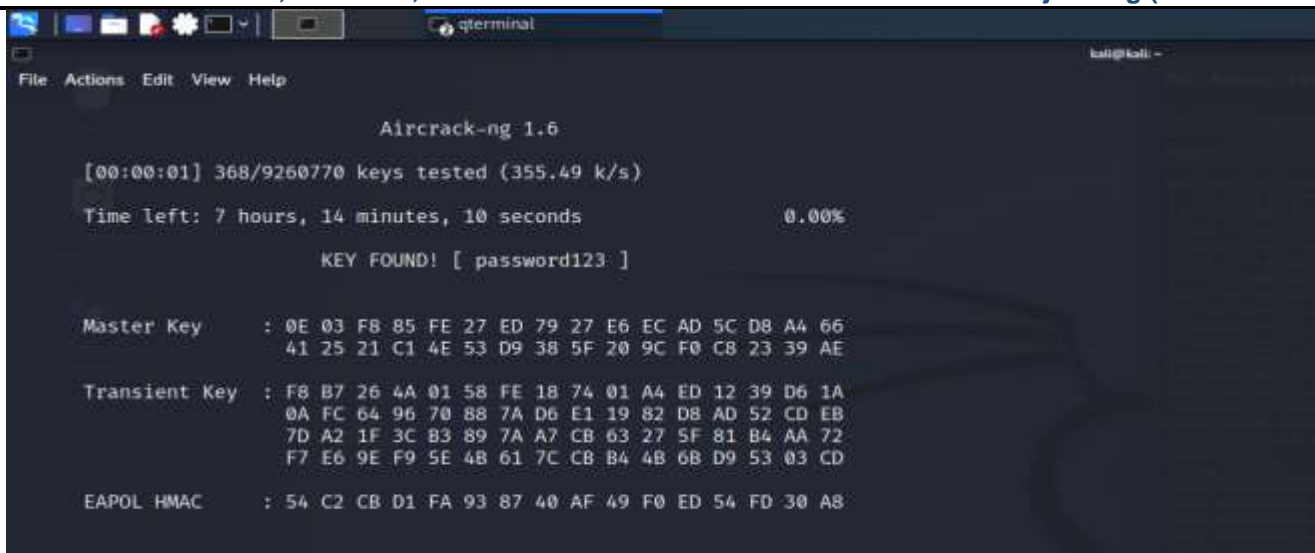
The result of this paper is, a vulnerability is found in the the Wi-Fi network that is being used and that allowed us to crack the WPA2 password. Penetration testing can be so helpful in testing a network to gather its weakness and think about its security like, not to maintain any weaknesses which can be attacked by hackers.

```

kali@kali: ~
└─$ sudo aircrack-ng handshake-wizard-01.cap -w /home/kali/wparockyou.txt

```

Fig 3: Working with handshake file and wordlist to crack the password



```

Aircrack-ng 1.6

[00:00:01] 368/9260770 keys tested (355.49 k/s)

Time left: 7 hours, 14 minutes, 10 seconds           0.00%

KEY FOUND! [ password123 ]

Master Key      : 0E 03 FB 85 FE 27 ED 79 27 E6 EC AD 5C D8 A4 66
                  41 25 21 C1 4E 53 D9 38 5F 20 9C F0 C8 23 39 AE

Transient Key   : F8 B7 26 4A 01 58 FE 18 74 01 A4 ED 12 39 D6 1A
                  0A FC 64 96 70 88 7A D6 E1 19 82 D8 AD 52 CD EB
                  7D A2 1F 3C 83 89 7A A7 CB 63 27 5F 81 B4 AA 72
                  F7 E6 9E F9 5E 4B 61 7C CB B4 4B 6B D9 53 03 CD

EAPOL HMAC     : 54 C2 CB D1 FA 93 87 40 AF 49 F0 ED 54 FD 30 A8

```

Fig 4: Result of penetration test i.e., the cracked password of the target network

### B. Discussions:

Penetration testing is often referred to as a "pen test" and is a testing procedure that is being performed to test the perimeters of a network for security breaches and vulnerabilities. Penetration testing is also known as ethical hacking because the test is performed by a team of security experts that have the organization's permission to hack the network in an attempt to identify the vulnerabilities in that network.

Penetration testing works on the premise that the hackers have more knowledge of network vulnerabilities than the organizations that run the networks, and they always stay a step ahead of the network experts. Therefore a team of network security experts to perform the tests using the same techniques that the hackers would use to breach network security.

Penetration takes the network security to next level by actually exploring the network for vulnerabilities. Simply deploying a firewall, a vulnerability scanner, and an antivirus program is not enough to protect the system against some attack.

When the penetration test is completely done, the security experts prepare a report for the organization that includes all the potential vulnerabilities in that network system. The report provides a way to evaluate the network system from an outside criminal's point of view so that the necessary steps can be taken to repair all that vulnerabilities and provide optimum network security.

## V. CONCLUSION

This paper aims to show how a network vulnerability is used to comprise the wireless network. We have done it by cracking the WPS enabled APs, capturing the handshake, creating a wordlist and at last by cracking the key. The main motive of this paper is to expose the dangers of public Wi-Fi networks used in our day-to-day life. Public Wi-Fi is usually untrusted and now no longer secure. People aren't advocated to connect to a public Wi-Fi, in particular for transaction or any interest that calls for touchy statistics. There are various other approaches that can be used to comprise a network. With the tremendous changes happening in wireless technologies, each and every individual must be aware of new attacks that are emerging, should safeguard themselves from such attacks and should know how to have a secured wireless communication.

## REFERENCES

- [1]. 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.
- [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]. McClure S, Scambray S J, Kurtz G, "Hacking Exposed: Network Security Secrets & Solutions", Chapter Wireless Hacking, Computing McGraw-Hill, 2012, ISBN-10: 0072121270
- [4]. The 10 Top Hacking Tools in Kali Linux, Hacking Tutorials (2015, July 16). Retrieved from: <https://www.hackingtutorials.org/wifi-hacking-tutorials/top-10-wifi-hacking-tools-in-kali-linux/>
- [5]. Roche M, Wireless Hacking Tools. Retrieved from: [http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless\\_hacking.pdf](http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking.pdf)
- [6]. Bradley M, (2017, June 9) "An Overview of Wireless Protected Access" 2. Retrieved from: <https://www.lifewire.com/what-is-wpa2-818352>
- [7]. 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>
- [8]. Mirjalili M, Nowroozi A, Alidoosti, "A Survey on Web Penetration Test", Advances in Computer Science: an International Journal, Vol. 3, Issue 6, 2014.
- [9]. Al-Ghamdi, "A Survey on Software Security Testing Techniques", IJCST, Volume 4, Issue 4, April 2013.
- [10]. Bishop M, "About Penetration Testing", IEEE Security and Privacy Magazine, 2007.