ETHICAL HACKING AND WI-FI HACKING

[1]*Shivam Kumar Jha,* [2]*Raj Dodiya*

[1]*Parul Institute of Computer Application, Parul University*
[2]*Parul Institute of Computer Application, Parul University*

[1]*shivamkumarjjha@gmail.com,* [2]*rajking3361@gmail.com*

Abstract: A permitted effort to acquire access to a particular system, business, or data is referred to as ethical hacking. Duplicating the techniques and behaviours of malevolent attacker is part of taking out for an ethical hack. The use of internet is increasing very fast and its use has increased even more, It is very helpful for us, due to which we can do many things just sitting at home and we do not need to go out, but Hackers are misusing the Internet for stealing people's personal information and using it for their own benefit by hacking the mobile phone, computer system and website of others, which causes a lot of trouble to those people and for many people, that's so we need Ethical hackers who have good knowledge about computer fundamental, operating system, computer networks, Programming Languages . Hacking Modules who can be able to save us from these attacks in This paper will discuss about hacking and how to stay safe from hacking we will discuss more about the security vulnerability and Ethical hacking.

Keywords: Ethical Hacking, Ethical Hacking Phases, Internet Security, Penetration Testing, Wi-Fi Hacking.

1. INTRODUCTION

The era of Ethical Hacking is spreading in every sector every industry doesn't matter that industry is related with IT or Not, security is necessary for every industry, organization or company because we live in the era of cyber-attacks, we all facing lot of cyber-attacks by black hat hackers, they steal private data and logs, technology is continuously increasing and we just independent on this technology [1]–[3]. The need of cyber expert who know very well how to defend it and how to preventing our personal data from the cyber-attacks.

1.1.What is Hacking?

Cyber - attack is the technique of finding potential security holes in a computing device in order to gain access too individually or collectively data, either ethically or unethically.

1.2.What is Ethical Hacking?

The motive of behind the hacking is totally depend to ethical hacking if that process is legal (Ethical) then he is Ethical Hacker he must have a Retain permission for penetrate on that system, server, company or any organization. If he has then and then he is Ethical Hacker otherwise we all know who that he a black hat hacker is.

1.3.Phases Of Ethical Hacking Process

- The Maintaining Access Phase
- The Clearing Tracks Phase
- The Scanning Phase
- The Reconnaissance Phase
- The Gaining Access Phase

1.4.About these phases

Every phase is same for all hacking process nothing change for any hacker, doesn't matter if any black hat hackers or gray hat hackers doing anything. Only one thing is changing behind that hacking. The motive of Hacking or Penetrating that computer system, web server, website, mobile phone or anything else.

- *Reconnaissance*

Reconnaissance Surveillance has been the process of enhancing information about someone or something, they using different ways different technique for gather information, from other resource about a computer system, server, website or anything else, and collect lot of information from others way then they will go for the next phases The Scanning Phases. The same process doing before penetrating any website or web server by penetration tester with ethically.

- *Scanning*

After the active reconnaissance, Scanning is the phase where attacker collect information directly, attackers identify useful information about the target like ports information, Address, operating system, active host, server, installed serves, vulnerabilities, bugs etc. then they go through that information to next phases where they Gaining Access.

- *Gaining Access*

After the scanning , they go for gaining access phases where they have already collect so much information about the target, because they already go with reconnaissance and scanning phases, they gain full access to that computer systems, networks, operating system or software At the computer system, application, network level, the attacker have full gaining access to yours device.

- *Maintaining Access*

After gaining full Access, there is another impotent step where we have to maintain the access. this is very impotent step because, if the user switch off his/her system than its difficult to gaining full access again and again it's better to maintain that access in most of the time attacker go with key logger, backdoors, rat, Trojans, payload, ransomware, rootkit, spyware, worm etc. they just go with any of these after that they have full access of your device for long and long time. Figure 1 discloses the maintaining access of the WI-FI system.

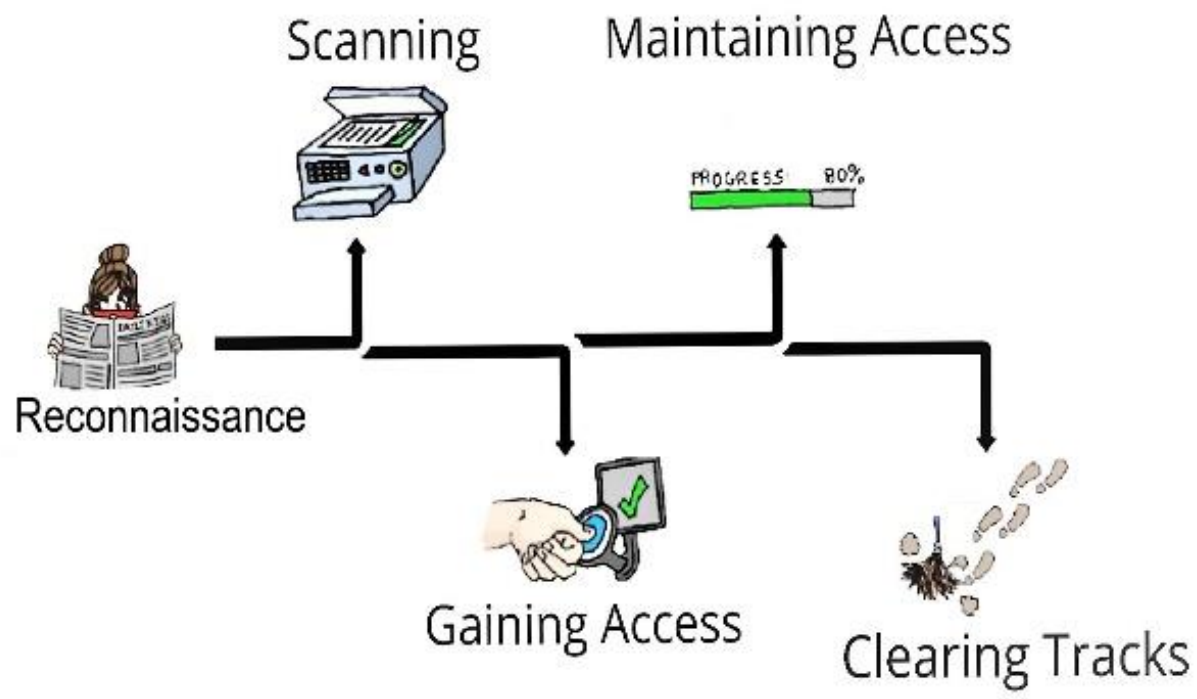

Figure 1: Illustrated the Maintaining Access of the System in the Particular Time.

- *Clearing Tracks*

On the last phase attacker erase all types of logs, malicious activity and everything related to that attack whatever they did with their server or system. At the other part penetration tester is doing same thing till now, at the last phases they have to submit their report on the basses of previous phases that process is known as “Reporting” to system or server owner.

- *Attacks in The Real Worlds*

How We Protect From These Hacking

- Attacks
- Update and always active your firewall/antivirus
- Use complex passwords
- Don't use same password Every Ware
- Use Multi-Factor Authentication
- Use good antivirus software
- Update frequently your apps, browser and operating system
- Don't share your personal information in social sites Use virtualization for browser surfing
- Take backup of your impotent data
- Never go to uneven site
- Enable encryption for all files
- Download apps/software from original resource (don't use crack software/apps it always comes with virus)
- Clear your logs and browser history .Figure 2 shows the different motivation by the different sectors.

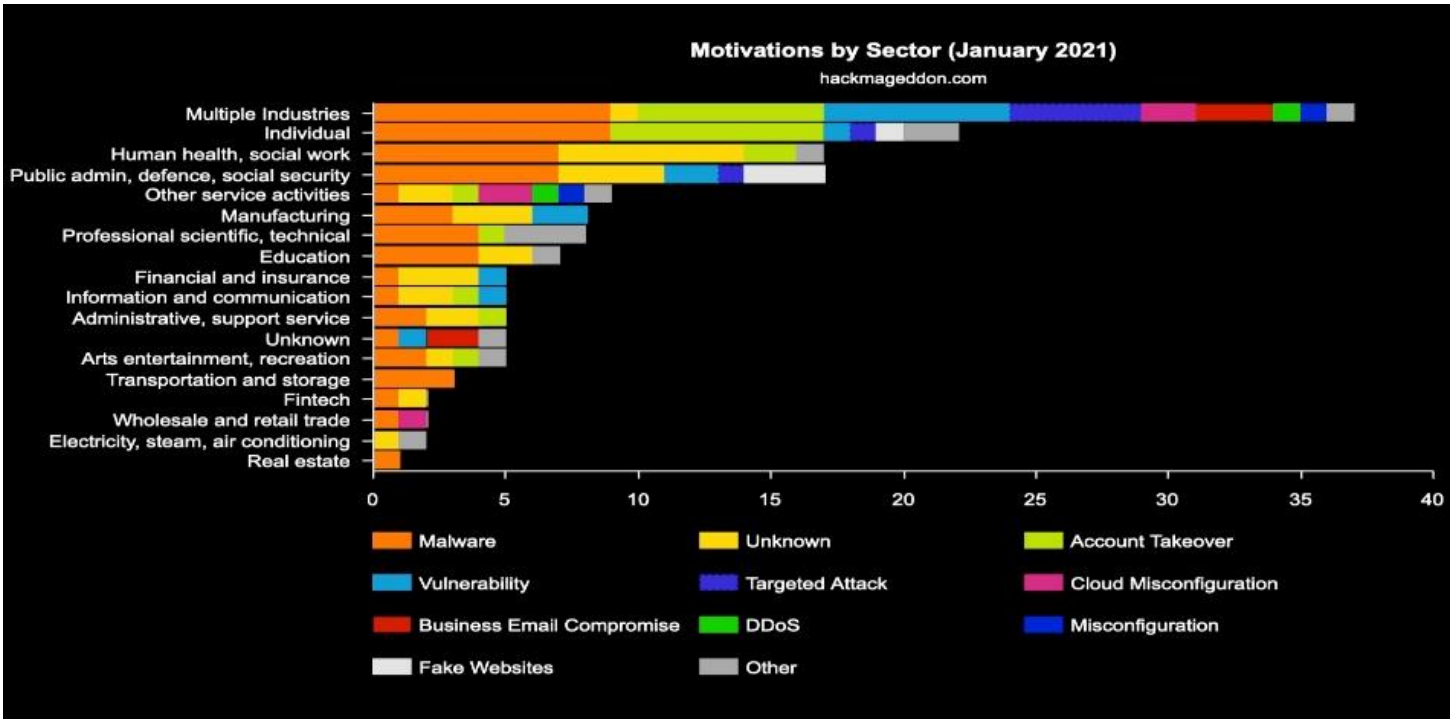

Figure 2: Illustrated the Motivations By the Different Sector of the System.

1.5.Why we should to go with Ethical Hacking?

- If you are expert in ethical hacking then you get lot of Global Recognition and fame in worlds
- If you are expert in ethical hacking then you going to earn good money
- If you are expert in ethical hacking then you defiantly get chance to work with Fortune 500 Companies
- Ethical Hacking is one of the most demanding skills.

1.6.Why We Should Not Go with Unethical Hacking?

Black hat hacking or Unethical Hacking is not recognise by anyone .If you earn good money with black hat hacking even then you going to punish by police or government If you chose black hat hacking then you have to always work alone

1.6.1. Wi-Fi Hacking

- *Risks of Using Public Wi-Fi Networks and more about Wi-Fi?*

The challenge with public Wi-Fi is that it come with a multiplicity of security dangers. While big businesses may believe they are providing a useful service to their consumers, the security on these networks is likely to be weak or non-existent. Since the initial days of something like the 802.11b architecture in the late 1990s, mobile hotspots have proven infamously unsafe [4]. Major 802.11 faults, including as fundamental security flaws, decryption flaws, and authenticity issues, have been uncovered since the standard's debut. Since then, wireless operations have always been on the rise. The situation is getting enough that severe that the Wi-Fi Affiliation has established two intrusion prevention standards and guidelines fight back against the aggressors. The Wi-Fi Secured Access (WPA) standard, which was established by the Wi-Fi Affiliation, represented as a temporary fix to a well WEP attack vectors it until IEEE released the 802.11i standard. This is now the approved Standard specification that includes the WPA patches for WEP, as well as various cryptographic procedures to make wireless networks even more secure.

- *Most common attacks*

- Jamming signals
- Unencrypted networks
- Malware distribution
- Misconfiguration Attacks
- Sniffing and snooping
- Malicious hotspots

1.7.Man in the Middle Attacks

One of its most prominent network threats is a person attacker. MITM attacks based on local area attacks. When Data travel from device to server and website. That time attacker tries to connect to that network from low vulnerabilities after that hacker has full access on that device, he controls every network packet.

1.8.What is Encryption?

The Encryption is process where the data sent from your device and was in a not in human readable form (secret) that can't be read by anyone who doesn't have the key to decode it. Encryption is switched off by normal with most routers when devices leave that factory, that's time must be activated on when the network is set up. If the network was set up by an IT professional, there's a high probability encrypted data was enabled. Yet, there is no best way to know if this has done [5].

1.9.What is WEP?

Wireless Equivalent Privacy (WEP) is a security approach for wireless devices. Their previous internet protocol, which was accepted in 1997, includes it. Its original goal as something of an early technique was to prevent Geezer attacks, which it did for a while. WEP encrypts all traffic with a 64 or 128-bit hexadecimal key. This is a permanent key, meaning means that independently of device, its same solution is used to encrypt all traffic. This protocol worked for a time until the computing power of regular devices became insufficient. Increased due to advances in IPC as well as slow processing frequencies when it was considered unstable, that protocol being decommissioned during this time.

2. DISCUSSION

2.1.What is WPA?

WPA is the abbreviation for "Wi-Fi Protected Access," as it's known. WPA (Wireless Protected Access) is a networked security standard for creating solid wireless broadband (Wi-Fi) communities. It's similar to the Standardized interview, but it's more advanced in terms of security keys and user permissions. For an encrypted transferring data to work, both workstations must utilise the same cryptographic key at the start and end of the transmission. WPA uses the While WEP utilizes so same key for all authorised platforms, the important considering integrity protocol (TKIP) contains high concentrations of the key utilized more by devices. Intruders won't have ready to invent their original secret information which might work only with insurance schemes. WPA additionally use the Extensible Authentication Protocol (EAP) for user authorization [6].

2.2.What is WPA 2?

WPA2 is an updated version of WPA that uses the resilient security network (RSN) technology. It was released in

2004. WPA2 has two modes of operation personal and enterprise. The home mode is designed for personal use, while the commercial mode is often utilized in a work environment. The AES-CCMP encryption method, which combines kept repeating with the CBC-MAC message authentication code approach and the AES block cypher, is used in both of these modes. Intruders snooping in on the connection will have a tougher difficulty detecting patterns as a consequence.

2.3.What is WPA 3?

This same Wi-Fi Organization claims that, WPA3 is currently regarded the necessary certification for Wi-Fi CERTIFIED devices. But what is WPA3 and how does it vary from its predecessors WPA2 and WPA? WPA3 intends to address some of WPA2's fundamental flaws. This allows it to provide greater security for personal and open networks, as well as enterprise network security advancements. WPA3 has the advantage of being resistant to brute force assaults, even with weak or short passwords. WPA3 Simultaneous Authentication of Equals (SAE), a secure password-authenticated key exchange technique, replaces WPA2-PSK. WPA3-SAE limits the number of guesses an attacker can make by not transmitting the password hash in clear text. Last year, though, researchers found a number of security issues.

2.4.Functionality of air crack-ng

Air crack-ng is a collection of tools for detecting flaws in Wi-Fi networks. It’s used to manage Wi-Fi security, capture datagrams, and translate them to text files that can be analysed.

It's used by pen testers to breach the WPA and WEP encryption. Air crack-ng is accessible with any network adapter controllers because driver implements raw monitoring mode. Aero crack-ng was created with Linux in mind, but it now works with Vista, OS X, Opens, FreeBSD, Solaris, NetBSD, and eComStation. It can use cyberattacks, PTW assaults, and the Fluhrer, Mantin, and Shamir (FMS) attack to break WEP keys, as well as decryption to crack WPA/WPA2-PSK keys. Select a Wi-Fi network that you have access to or have permission to use, and then launch Air crack-ng to disclose the password (Figure 3) [7], [8].

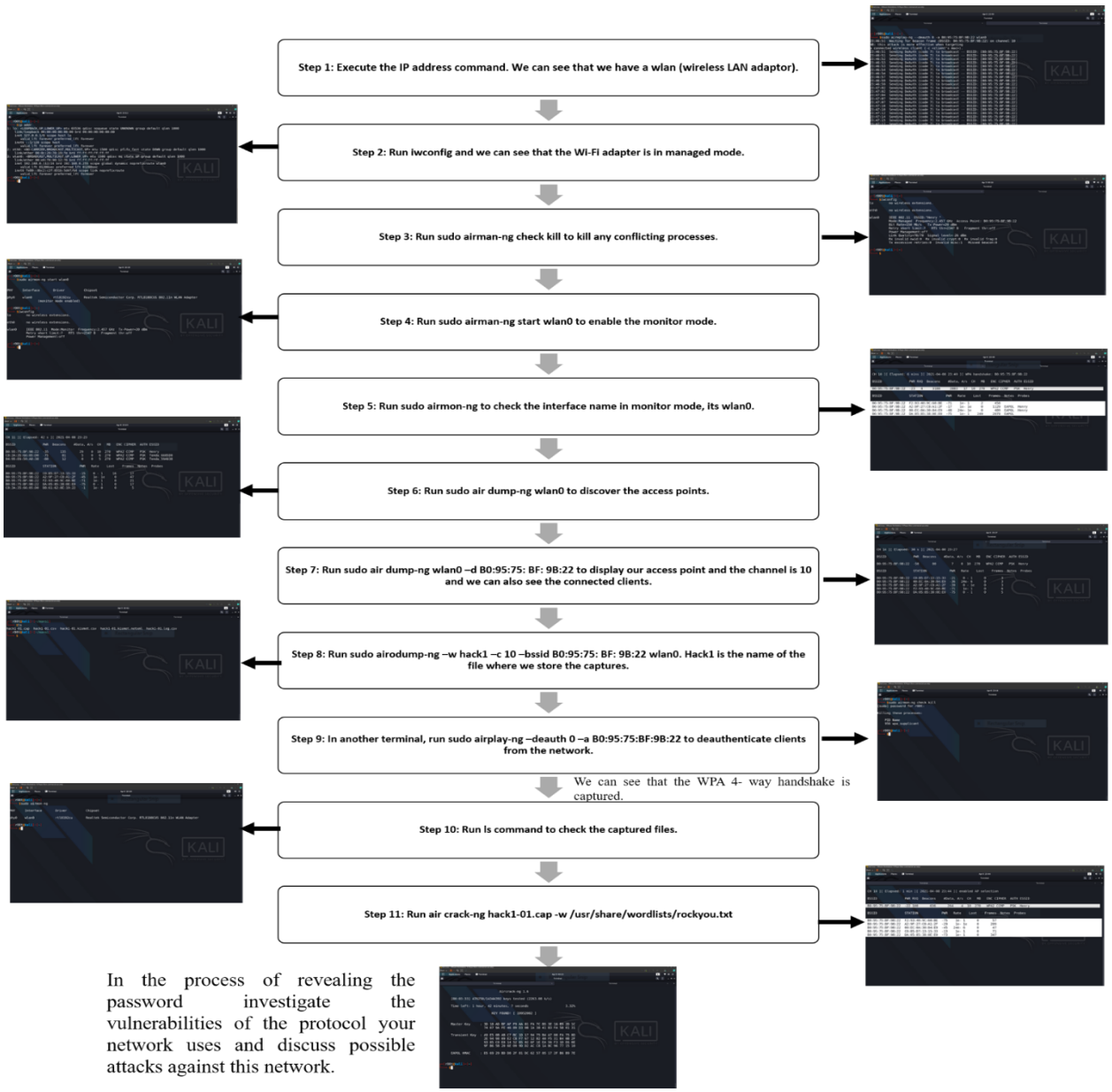

Figure 3: Illustrating the Various steps of the Process

2.5.Default Password or SSID

If the router or wireless access point (A default)'s SSID, such as Linksys or Delink, is changed, it increases the chances that anyone can crack the Wi-Fi password. This is because dictionary-based cracking relies on the SSID, and using a default or standard SSID makes things a little easier.

2.6.APs and hardware network are not physically secured

The authentication measures can be rapidly bypassed if someone has physical access to the wireless access points or other network devices. If your AP is on a table in an unlocked room, for example, a guest may easily reset the access point to its default settings, allowing unsecured network access.

2.7.Authentication via WPS PIN

When using the personal mode of encryption, a flaw in the WPS PIN authentication method allows others to break the 8-digit PIN and recover the password, allowing them access to the network.

2.8.Execution plan and results

The plan called for using a variety of Linux tools to crack the wireless network's password.

The WPA2 key was extracted from the rock you.txt file after capturing the four-way handshake.

2.9.F. Analysis

We analysed at how the 4-way handshake works and what the WPA/WPA2 protocol's vulnerabilities are. We learned how to crack WPA/WPA2 keys using a variety of techniques. To record packets and traffic for a specific wireless device, we can switch to monitor mode. We can also de-authenticate the connected clients before cracking the wireless network's password with the air crack tool [9].

3. CONCLUSION

In a sense, any wireless network can be attacked in a variety of ways. Potential vulnerabilities include using the default SSID or password, WPS pin authentication, inadequate access control, and leaving the access point accessible in unlocked locations, all of which can lead to data theft of critical information. The architecture of kismet in WIDS mode may protect the network from DOS, MiTM, and MAC spoofing attacks. Regular software upgrades and the usage of firewalls, on the other hand, may assist protect the network from external intruders. Ethical hacking is the practice of identifying problems in a service, system, or institution's infrastructure that may be inject malicious code. By legitimately breaking into networks and searching for weakest places, they employ this approach to avoid invasions and privacy violations.

REFERENCES:

[1] D. Jamil and M. N. A. Khan, “Is Ethical Hacking Ethical?,” *Int. J. Eng. Sci. Technol.*, 2011.

[2] R. Hartley, D. Medlin, and Z. Houlik, “Ethical Hacking: Educating Future Cybersecurity Professionals,” *Proc. EDSIG Conf.*, 2017.

[3] C. C. Palmer, “Ethical hacking,” *IBM Syst. J.*, 2001, doi: 10.1147/sj.403.0769.

[4] H.-R. Bae, M.-Y. Kim, S.-K. Song, S.-G. Lee, and Y.-H. Chang, “Security Attack Analysis for Wireless Router and Free Wi-Fi Hacking Solutions,” *J. Converg. Cult. Technol.*, 2016, doi: 10.17703/jcct.2016.2.4.65.

[5] Z. Zhou, C. Wu, Z. Yang, and Y. Liu, “Sensorless sensing with WiFi,” *Tsinghua Sci. Technol.*, 2015, doi: 10.1109/TST.2015.7040509.

[6] D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti, “BackFi: High Throughput WiFi Backscatter,” *Comput. Commun. Rev.*, 2015, doi: 10.1145/2785956.2787490.

[7] Y. He, M. Chen, B. Ge, and M. Guizani, “On WiFi Offloading in Heterogeneous Networks: Various Incentives and Trade-Off Strategies,” *IEEE Commun. Surv. Tutorials*, 2016, doi: 10.1109/COMST.2016.2558191.

[8] D. V. Kondrat, “Factors influencing consumer behavior,” 2016. doi: 10.21661/r-80748.

[9] M. (2012). Bansal A.& Arora, “Ethical Hacking and Social Security. Radix International Journal of Research in Social Science”.