INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 08, August 2023, pp : 72-75

e-ISSN : 2583-1062

Impact Factor : 5.725

WIRELESS NETWORK PENETRATION TESTING

Abid Salam[1], Dr. Nitin Kumar[2]

[1]M. Tech Scholar, Ganga Institute of Tech. & Management, Jhajjar, India.

[2]Assistant Professor, Ganga Institute of Tech. & Management, Jhajjar, India.

ABSTRACT

Wireless networks have become an integral part of our daily lives, providing convenient and ubiquitous connectivity. However, the widespread adoption of wireless technologies has also introduced new security risks and vulnerabilities. Wireless penetration testing is a critical process that aims to assess the security posture of wireless networks by simulating real-world attacks. This abstract explores the concept of wireless penetration testing, its objectives, methodologies, and tools used in the process. It emphasizes the importance of identifying and mitigating potential security vulnerabilities in wireless networks to protect sensitive data and ensure the integrity and availability of network resources. The abstract discusses various wireless penetration testing techniques, such as passive and active reconnaissance, wireless network scanning, encryption cracking, and exploiting weak authentication mechanisms. It also highlights the significance of understanding the specific security protocols and standards employed in wireless networks, such as Wi-Fi Protected Access (WPA) and WPA2, and the implications of vulnerabilities in these protocols. Furthermore, the abstract addresses the legal and ethical considerations associated with wireless penetration testing, emphasizing the importance of obtaining proper authorization and ensuring compliance with relevant laws and regulations. It also highlights the need for ongoing monitoring and periodic re-assessment to address emerging threats and evolving security landscape. By conducting wireless penetration testing, organizations can proactively identify and address vulnerabilities in their wireless networks, enhance their security posture, and prevent unauthorized access, data breaches, and other malicious activities. The abstract concludes by emphasizing the critical role of wireless penetration testing in maintaining a robust and secure wireless network infrastructure in today's interconnected world.

1. INTRODUCTION

The first Wi-Fi 802.11 wireless standard was created in 1997. In less than 20years, the data transfer speed increased from 1 Mb/s to an incredible speed of 6.75 Gb/s. Over time, Wi-Fi has penetrated a large number of companies, schools and households. Based on research from 2011, every fourth household has its own Wi-Fi network. More developed countries such as Germany and France reach over 70% household coverage.[1]According to predictions, there will be over 20 billion devices connected to the Internet by 2020, most of which will be connected wirelessly.[2]Wireless technologies, including Wi-Fi, are therefore still in development and their popularity is increasing every year. However, in addition to the benefits of Wi-Fi networks, their negative aspects must also be taken into account. One of these negative aspects is security. With classic cable networks, data travels only through the given medium-the cable. This data transfer is relatively safe, since the only way to steal it is through a direct physical connection to the network. However, in the case of Wi-Fi networks, the transmission medium is air. Data is flying all over the place, so anyone within signal range can theoretically capture and read it. Due to this fact, a number of security issues arise that must be addressed when using Wi-Fi networks. The aforementioned growing popularity of Wi-Fi networks and various security threats became the motivation for developing this work. Countless researches prove every year that ordinary users do not care much about their protection on the Internet. We therefore researched what threats users are really exposed to and what they are at risk of on Wi-Fi networks. However, we looked at security issues from a slightly different perspective. Instead of securing networks, we tried to disrupt their security. In the following document, we therefore describe different types of cyber attacks against Wi-Fi networks. We are not only dealing with attacks on a theoretical level, but all types of described attacks have also been carried out practically. We used the same tools used by professional security analysts and hackers to carry out the attacks. After carrying out these attacks, we subsequently proposed measures that would prevent similar attacks in the future.

2. OBJECTIVES

The main goal of the work is to demonstrate the potential danger on Wi-Fi networks. The work will focus on the practical execution of the attacks mentioned so far. Each such demonstration will be documented in detail from a theoretical as well as a practical point of view. We will then compare the attack with other attacks of a similar type and at the end we will evaluate which of the attacks is the most effective for solving the given situation. Various aspects will be compared, especially the time required, the probability of success, the knowledge required and other special requirements necessary for the implementation. In the case of attacks in a theoretical form, their usability in real pg. 9 conditions will be discussed. After the successful completion of all tests, solutions will be proposed that could repel individual attacks, or at least mitigate their negative consequences for user security and the smooth operation of the computer system. After all the tests are completed, a document will be released that summarizes all the solutions so far and interprets them in a less professional form for ordinary users, who will be advised how to properly secure their home Wi-Fi network. The second document will cover various techniques for protecting user data while using public Wi-Fi networks. After completing the practical tests, we will continue to deal with the topic of minor research. Through a short internet questionnaire, we will evaluate the security habits of users of Wi-Fi networks in Slovakia. To get objective results, we will need at least 200 respondents, which we will try to get with the help of social networks and Internet discussion forums. We will process the survey results in the form of Excel tables, graphs and dependencies. We will evaluate these results and then compare the security habits of individual age groups, as well as based on the relationship of individuals to information and telecommunication technologies We will try to publish the results of penetration tests, prepared documents on the topic of security improvement, and survey results. These publications will be mainly aimed at educating ordinary users about cyber security, and thus also increasing their prudence when using information technology.

3. METHODLOGY

3.1 Preparing to carry out attacks

Both software and hardware preparation are necessary for the successful execution of various tests. From the hardware side, we need at least 1 Wi-Fi router, which we set during attacks to simulate the desired situation. Next, we need several wireless devices that will act as clients on the network. The most important device should be a powerful laptop, with which the attacks will take place. We also need specialized software to carry out the described attacks. Practically, any Linux distribution of the operating system is enough for us. However, to simplify the process, we will use distributions that have built-in various tools for performing penetration tests. One such system is Kali Linux, which we will use in the course of this work. From the official site kali.org it can be downloaded for free under the GNU GPL license. After downloading, it is necessary to install this image either on a physical or on a virtual computer. For the purpose of our tests, we used the installation directly on a physical computer, thus creating a dual-boot system. After installation, we updated and upgraded the system. pg. 10 After all the software preparations, we started and set up the afore mentioned WiFi routers. Subsequently, cables were connected and clients were connected to the network. The process of simulating attacks could thus begin. In normal Wi-Fi mode, the adapter captures only the communication that is intended for the given device. However, we used the air mon-ng program, which enables easy switching of the interface to monitor mode. In this mode, the Wi-Fi card tries to capture all surrounding communication, which is a necessary element for most Wi-Fi attacks.

3.2 Carrying out attacks on WEP networks

As we mentioned in the theoretical part, the WEP protocol is outdated and can be broken in a few minutes. In our tests, various types of WEP attacks were used, but they all had the same goal to obtain the largest possible number of initialization vectors. One way to achieve this state is through a passive network monitoring attack. If there are clients on the network that are actively communicating with the network, each of their messages is encrypted with a new initialization vector. Depending on the number of clients and the type of their communication, it is possible to obtain a sufficient number of IVs within a few tens of minutes. We used the integrated Wi-Fi network to monitor and capture communications. We used the PTW method and the air crack-ng program for the statistical analysis of the captured data. However, the passive method of attack takes a lot of time, so in the next tests we started with a slightly more aggressive style. One of the more aggressive ways to get a large number of IVs in a short time is an attack called ARP Replay. In this attack, we intercepted the ARP request and re-posted it to the network using the air eplay-ng tool. The intercepted ARP packet still had to be modified so that the current destination MAC address was replaced by the broadcast MAC. This address has the form FF:FF:FF:FF:FF:FF and we achieved its change using the programs air eplay-ngand packet forge-ng. We will then push such a packet onto the network. Since it is a broadcast address, all devices on the network forward this packet, always encrypting it using a different initialization vector. Thus, we forced the devices to generate new IVs, which greatly accelerated the attack. Other types of attacks a real so based on the generation of broadcast ARP messages, but achieving this process is also possible in other ways. We also used the air crack-ng toolkit to perform additional attacks.

3.3. Brute-force attack against WPA/WPA2

The basic need for brute-force WPA attacks is to capture 4-way handshake messages between the access point and the client. These messages can be captured using various packet sniffing programs, and in our tests we used the air odump-ngtool. Air odump-ng automatically writes captured data to a file and prepare sit for later analysis. With the air eplay-ng program, we then caused the client to be de authenticated from the network, causing it to re-authenticate and start the 4-step message exchange process. OurWi-Fi adapter caught this process and successfully wrote air odump-ng packets to disk. In order to perform a brute-force attack, we also needed a word data base from which words are read during the brute-force. These databases are freely available on the Internet. Word databases of several gigabytes can be downloaded through various sites, forums, and torrents. In our tests, however, due to time constraints, we used only 2 databases with a size of 150 megabytes each, with a total volume of over 30 million words. All these words were subsequently inserted into the hash function in order to reveal the password.

However, this program can only use CPU processing power. For acceleration, we used the computing power of the graphics unit of a desktop computer in the next stages. We used a specialized program for this purpose.

3.4. Exploitation of WPS vulnerabilities

Attacks on networks with WPS support must also be carried out using specialized software. In our case, we used the Reaver and Bully programs, which more or less automate the whole process. The programs began to attack the desired network immediately after providing the necessary arguments. These arguments included the MAC address of the access point, the channel on which it broadcasts and the possible specification of some timeout values. The attack consisted of guessing individual WPS PIN codes from1111 111 to 9999 999, while the last digit was always added. During an attack on the Cisco EPC3925, a potential attack was detected and the WPS function was intelligently locked. We tried to restart the device through a DDoS attack, which would unlock the WPS function again. For this purpose, we used the mdk5 program, or we tried to use other scripts to automate this process.

Unfortunately, we were not able to implement a Pixie Dust attack in practice, because we did not have any equipment at our disposal that would be susceptible to this type of attack.

3.5. Interception of wireless communication

We used the Wire shark program to capture and process captured wireless messages. After turning on the program, we specify the interface that will capture packets. Before that, this interface must be placed in monitor mode to capture all wireless communication. Placing in monitor mode can be done using the air monng program, or by a sequence of the following commands:

```
ifconfig wlan0 down &&iwconfig wlan0 mode monitor &&ifconfig wlan0 up
```

After setting the monitor mode, check the monitor mode button directly in the program and we can start data capture. Capture messages from WEP and WPA networks is not yet possible, as this data is automatically encrypted. However, if the access key is known, it is possible to define in the Wire shark program that the intercepted communication is directly decrypted. We set this process in the section Edit- >Preferences-> Protocols -> IEEE 802.11.

3.6. Preparation and processing of the questionnaire

After lengthy negotiations, we managed to make an agreement with the IT portal. This agreement was aimed at the implementation of an internet poll and the subsequent publication of its results. The questions used in the questionnaire can be found in the appendices. After the survey, we imported the obtained results into the Excel program. As a result, we created tables with answers, which, however, had to be processed in some way. Part of the processing was the filtering of some records that were evaluated as invalid using our algorithms. In the survey, we used control questions that monitored whether the respondent really fills out the survey or whether he just randomly clicks on the first option that comes to hand. These algorithms examined the relationship between these control questions and the respondent's answers. In case of different answers to the original and control question, points were added to the respondent, while upon reaching a certain number of points, the algorithm evaluated the records as invalid. By using this system, we achieved greater objectivity of the final results. After filtering inappropriate records, we further evaluated the survey results. We used Excel functions for evaluation, the most common were COUNTIF, IF, AND, OR, etc. We created various graphs and dependencies from the created tables. However, there were too many of these graphs, so by creating our own algorithm, we made the so called " security index", which is actually a real number ranging from-13.9 to 8.05. This number scores the individual questions and the relationships between those questions in the survey. The resulting pg. 13 value of the index expresses the comprehensive value of an individual's security. A higher number means better security, while a value below -0.45indicatesinsufficient security of the respondent.

4. CONCLUSION

In this work, we have successfully demonstrated penetration into networks using different security standards. We were able to crack the WEP protocol within minutes. These tests confirmed the previously known facts about the vulnerability of Wi-Finetworks with support for WEP encryption and further strengthened our belief that the WEP security protocol should no longer be present in today's networks. Further tests on networks using WPA and WPA2 protocols confirmed that, if a strong password is used, network soft his type are almost in vulnerable. However, the only threat to these networks can be the WPS system, which is implemented on most devices from the factory. The WPS protocol can be easily abused by a classic brute-force attack, and therefore were commend disabling it. Most of the attacks exploiting WPA TKIP encryption are still only in theoretical or experimental form, but we, through the hackforums.net community, have joined a project to develop a tool that would allow such an attack. The tool is currently in the alpha version, but one of our D-link type routers succumbed to this attack and we were able to successfully push 4 packets onto the network via QoS channels. This type of attack is very time-consuming and the network must meet several conditions to carry it out, so the attack is inapplicable in some cases. Based on these facts, we do not expect this type of attack to succeed. For these reasons, WPA networks are still relatively secure.

5. REFERENCES

[1] M. Ghavami, L. Michael, and R. Kohno, “Ultra Wideband Signals and Systems in Communication Engineering,” 2nd ed., John Wiley & Sons, pp. 166-174, 2007.

[2] G. Kumar, and K.P. Ray, “Broadband Microstrip Antennas”, Artech House, Inc. Boston, London, 2003.

[3] C. A. Balanis, “Advanced Engineering Electromagnetics,” 2nd ed., John Wiley and Sons, New York, 1989.

[4] R. Garg, P. Bhartia, I. Bahl and A. Ittipiboon, “Microstrip Antenna Design Handbook,” Dedham MA, Artech House, Inc. Canton Street, Norwood, 2001.

[5] N. Ida, “Engineering Electromagnetics,” New York, NY, USA: Springer, 2015.

[6] D. G. Fang, “Antenna Theory and Microstrip Antennas,” CRC Press, Boca Raton, 2006.

[7] I. J. Bahl, and P. Bhartia, “Microstrip Antennas,” Artech House, Inc. Boston, London, 1980.

[8] C. R. Johnson and H. Jasik, “Antenna Engineering Handbook,” 3rd ed., McGraw-Hill, New York, 1984.

[9] K.C. Gupta, R. Garg, I. Bahl, and P. Bhartia, “Microstrip Lines and Slot lines,” 2nd ed., Artech House, Boston, London, pp. 122-132, 1996.

[10] Y. Huang, and K. Boyle, “Antennas: From Theory to Practice,” John Wiley and Sons, New York, 2008.

[11] G. A. Deschamps, Microstrip Microwave Antennas, 1953, presented at Proc. 3rd USAF Symposium on Antennas.

[12] R. Munson, \Conformal microstrip antennas and microstrip phased arrays," IEEE Transactions on Antennas and Propagation, vol. 22, no. 1, pp. 74{78, 1974.

[13] J. Q. Howell, \Microstrip antennas," IEEE Transactions on Antennas and Propagation, vol. 23, no. 1, pp. 90{93, 1975.

[14] R. Garg, P. Bhartia, I. Bahl, and A. Ittipiboon, Microstrip Antenna Design Handbook, ser. Antennas and Propagation Library. Artech House, 2001, ISBN:9780890065136.

[15] J. W. Wallace, M. A. Jensen, A. L. Swindlehurst, and B. D. Je_s, \Experimentalcharacterization of the mimo wireless channel: Data acquisition and analysis,"IEEE Transactions on Wireless Communications, vol. 2, no. 2, pp. 335{343, 2003.