**De Authentication Attack: A Review**

Tushar Rakhra1, Arjit Kaushal2, Sarvesh Tanwar\*3, Priyanka Datta4, Ajay Rana5

*1,2,4 Chitkara University Institute of Engineering & Technology,*

Chitkara University, Punjab, India

3,5Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida

[tushar1611.cse18@chitkara.edu.in1](mailto:tushar1611.cse18@chitkara.edu.in1), [arjitrocks1999@gmail.com2](mailto:arjitrocks1999@gmail.com2),

[s.tanwar1521@gmail.com](mailto:s.tanwar1521@gmail.com)3, [priyanka.datta@chitkara.edu.in4](mailto:priyanka.datta@chitkara.edu.in4), 5ajay\_rana@amity.edu

***Abstract***

Nowadays people have so many smart devices that are connected to their Wi-Fi access points for access to seamless internet service. The data transfer between the device and access point has to be at utmost security so that one may not lose their data or access to their device a hacker can simply intervene in this process of data sharing and can have access to your device.de authentication attack is one such process in which the hacker creates fake access point of data and lures you into to access it as soon as you connect to it he has the access to send you content which can further help him stealing vital and information. In this paper we have done a complete research analysis of how the society faces challenges from hackers. we have collected data and studied how many big companies are facing hard challenges to keep their data secure. We have also discussed DE authentication attacks in this paper, which is important for many other attacks such as for breaking WPA or WPA2 security.

***Keywords:*** Cyber-attacks, Hacking, Ethical Hacking, Malicious Hackers, DE authentication attacks.

**I. Introduction**

Most of the work in today’s day to day life is done online. Myriad people these days have their private or sensitive data online. Due to this approach of people depending so much on network and internet, it has given hackers a new boon. Hackers try to access such data with or without the knowledge of the user. There are mainly two types of hackers one’s which do not follow rules and others which follows the rule that is ethics.

Almost every companies and big domains have sensitive and confidential data, which are available online. The person who can access this data without the knowledge or permission of the corporation will be known as a hacker, although hackers might be of two types one which uses his skills of hacking to protect the data of such companies and other who uses his knowledge to hack into such companies. So basically, we can categorize hacker under two main categories

*1. Ethical hackers*

These are the hackers which work under ethics, i.e. to protect a network from getting hacked. They do not hack with malicious intent; in fact, they work for the betterment of security of networks.

*2. Malicious hackers*

These are also known as black hat hackers or criminal hackers. They usually hack into computers or networks to steal information

Hacking is basically defined as breaking into the system and controlling it without the knowledge of

the owner i.e., stealing information like credit card numbers, phone numbers etc. The hackers hack such information for their own use and with malicious intent. This era is called the “secure era” not because of everybody’s awareness of security but because of the need of it. Since the explosive growth of internet, the e-commerce sites and the online usage has increased sufficiently which have given hackers more clients to break the security.

There are different definitions of hackers previously hackers were known as talented individuals who know stuff about computer more than average people, but now a hacker may be defined as an individual who can penetrate security and access computers beyond the restrictions on the other hand ethical hacking may be defined as a process in which an individual hack into a system with the permission of the owner for checking the systems’ security. Hackers can be categorized also as black hat, white hat, and grey hat hackers. Black hack hackers are the one’s which hack for malicious purposes, White hat hackers are the one’s which hack for the security of a corporation or with permission of the owner they are trying to hack, Grey hat hackers are the combination of both black hat and white hat hackers.

The target of this paper is to research an extraordinary Denial of Service (DoS) attacks on remote networks [11][12]. This assault is known as the DE authentication attack which is dispatched against remote organizations. At the point when a customer needs to detach from the remote passageway, it sends exceptional casings known as de-authentication or disassociation outlines. Due to being scrambled, these casings don't require a verified client [14]. Thus, an assailant can create these casings and send them to the passageway in such a way that the passageway expects the casings to be originating from the customer and not the assailant [13].

**II.MOTIVATION** Nowadays many companies suffer losses due to security breaches loss of personal data, professional data; banking information etc. to hackers is very pain full for such companies who have put years of hard work to collect this. hackers sell this precious data in black market or use it threaten the companies or simply leak over the internet to seek attention of the public. This is the prime reason to write this paper to tell about the loss incurred due to de authentication and ethical hacking by these giant’s firms and also tell about importance of ethical hacking and ethical hackers in such a world where no data is safe.

**III. Literature Survey**

In this section we described the work done by other researchers.

**Table 1: Literature Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sr No | Author | Year | Brief summary of their work | Future Scope |
| 1 | Wang and Yang [8] | 2017 | In this review paper, they had analyzed the art of vulnerable scanning tools which are open source. An environment of virtual lab had been introduced for designing their research lab. OpenVAS, a vulnerable scanning tool has been used along with the designed hands-on lab. Hands-on-lab on Cybersecurity plays a very vital role in making student aware about the idea and concept of ethical hacking. Tools used in the hands-on-lab are OpenVAS and VirtualBox along with Nmap, since they are available as open source and helps students for achieving their learning objectives. | Design of more Hands-on-labs with various types of vulnerable scanner which are available free, so that students can analyze their result and understand how hackers does their work before attacking. |
| 2 | Kumar et. al. [9] | 2015 | In this paper a conference was held which included about 206 IT security professionals who were interviewed and were asked to present their views on the topic of ethical hacking. All of them agreed that “ethics” is the key to prevent all the risks which students may possess if they work illegally. Many methods were suggested by IT professionals  They are as follows   * SOCIAL INTERACTION * COMPETITION * RECOGNITION * ONGOING SKILL DEVLOPMENT |  |
| 3 | Neeraj Rathore [15] | 2016 | This paper explores the fast-growing Cyber world and its components over the internet. It is also highlighting the role of ethical hacker to evacuate from the culprits and cybercrime and illustrate on proactive approach to minimize the threat of hacking and Cybercrime. | Some precaution and proactive action can eliminate the hazard and cyber terrorism. |
| 4 | Harry Gunrato |  | The recent world of information society with global cyberspace and networks will inevitably generate different types of political, social and ethical issues. Many complications in relation to human relationships and the society become apparent, when maximum human activities are done on cyberspace. Some fundamental ethical problems due to the use of Internet technology globally consist of personal private data, access rights of data, and destructive actions taken place on the Internet. These fundamental issues have solved partially with the use of emerging technology such as SSL, encryption technique, computer firewalls and digital IDs. Along with these protection technologies, some legal laws are also required in cyberspace to solve many issues related to cyber space of countries, which are linked into one global network. Strategies and guidelines should be executed so that global data can be used in an ethical way for future applications and benefits. |  |
| 5 | Michael and Guest [16] | 2016 | This research paper portrays the utilization of manufacture your own ethical hacking simulations to help learners for understanding penetration testing procedures. Senior level college understudies of ethical hacking class were given entrusted like the improvement of a catch with the utilization of flag platform that give scored to the members' advancement while misusing a vulnerable web site. | The development of a fetching storyline for the participant is the main aspect of this system. |
| 6 | Trabelsi and Ibrahim [17] | 2013 | Denial of service attacks are one of the main components of ethical hacking. Three different types of dos attacks are discussed in this paper. This paper discusses how to teach students to implement these attacks in an isolated network environment. It also discusses some issues and problems in teaching of ethical hacking and then lists the points with which students of schools can have successful implementation of such attacks. The paper explains three types of classical dos attacks, such exercises are developed to be included for intrusion detection and ethical hacking. Some issues have been raised on the matter of how ethical hacking has been taught inside the schools or organizations. | However, the ethical concerns of  teaching students “hacking” are dwarfed by the need for  knowledgeable, competent, and, above all, experienced  Computer security professionals. To reduce the schools and  educators’ liabilities, the paper lists a number of steps that should be taken when teaching ethical hacking techniques.  Schools that take the listed steps improve the chances of having  a successful and problem free information security programs  that teach offensive techniques. |

**IV. OBJECTIVE**

This paper aims to spread awareness about ethical hacking and how it affects people. In recent years’ technology has proved to be a boon with some bane’s too. We can’t rely too much on security as we come to know through this paper that security can be compromised easily. This paper shows how much security breaches occur throughout different devices and also through different types of organizations.

**V. EFFECTS OF HACKING**

Top cyberattacks which ruined many companies [12]**:**

* **ADOBE**- This Company has gone through a very tough time as in October 2013, some 2.9 million accounts were stolen from their database which led to leakage of their (logins, password, names, credit card numbers and expiration dates). Hackers took advantage of the security breach. adobe also lost their product data like some of it was of famous adobe photoshop, cold fusion, etc.
* **SONY** – This was loss to the biggest console making Sony as Sony’ s famous plays station network was attacked, and they lost about 77 million user data and banking information of many was comprised. After this they shut the server down for 1 month to get it fixed. This humongous loss was due to a simple SQL injection.
* **TARGET** – it is the second largest US retail chain got caught by a cyber-attack in December 2013. About 110 million customers lost their personal data. the attack was so beautifully executed that the company didn’t even in knew that they had lost so much thanks to American security services they told the company that they had compromised so much data. It led was to loss of 18 million dollars to company.
* **HOLD SECURITY**- it’s a shameful thing to say but such a reliable IT security company to lose about 1.2 billion logins, and passwords of about 420,000 websites around the world. Hackers introduced programmed botnets to visit sites and perform vulnerability tests in order to exploit SQL injection.
* **YAHOO THE FAVOURITE**- This company is hacker’s favorite and they have acquired about 3 billion user accounts from them in 2013.

**VI. METHODOLOGY**

Applications of de-authentication attacks-

*1. Evil twin access points*

De-authentication attacks are mainly used to disconnect the client from the main access point, so that to force them to connect to an evil twin access point. By this way the hackers can capture the packets transferred between the client and the access point

*2. Password attacks*

to initialize a brute force or dictionary attack on a client connected to an Wi-Fi with WPA or WPA2 enabled, a hacker has to capture a WPA 4 way handshake. The user can be forced to connect again and provide a 4-way handshake.

**VII. RESULT ANALYSIS**

Steps for de authentication attacks:

The two main things we must know are:

a. The device to be disconnected

b. The router that the device is connected to it is done using kali Linux operating system

1. First we will use the command: - airodump-ng wlan0(wlan0 Is the name of the wireless router of the hacking device)

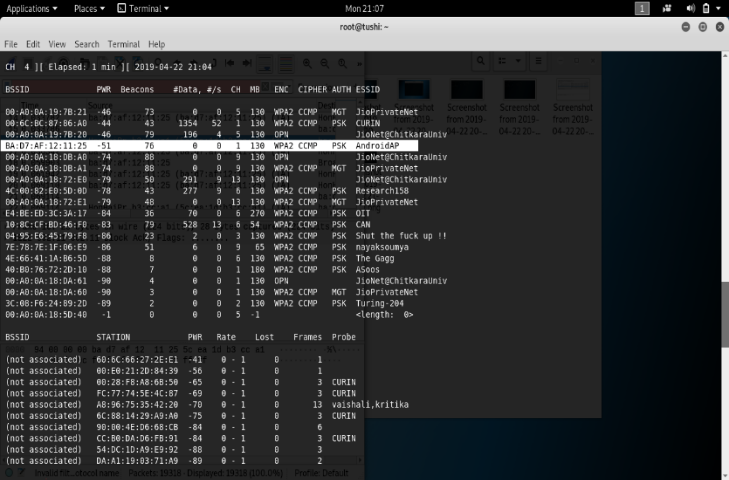


Figure 1: All the wireless networks available to be connected are displayed

By using this command, we can see all the network routers in range. this step is important as through this step only we will come to know about:

* The BSSID (mac (media access control) address of the router)
* The channel for the router

In this case the victim (client) is on the network AndroidAP so we’ll note the BSSID and The Channel for this router.

2. We’ll use the command airodump-ng --BSSID [router’s BSSID] --channel [router’s channel] wlan0

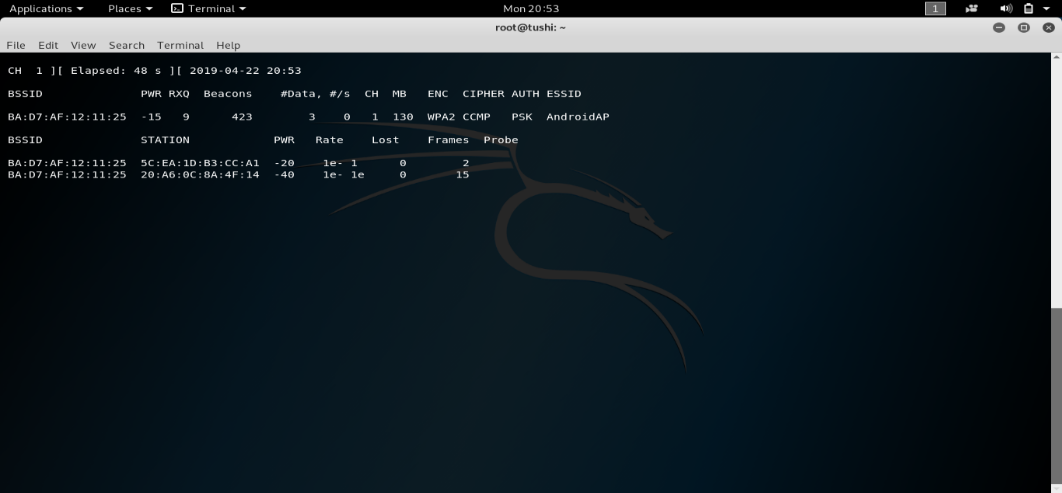


Figure 2: The specific network to which the victim is connected is shown in detail

By using the above command, we can see all the devices connected to the target network. although we cannot see the specific device as we do not know which device which mac address has so we will save the following data in Wireshark

3. airodump-ng --BSSID [router’s BSSID] --channel [router’s channel] –write [file name] wlan0

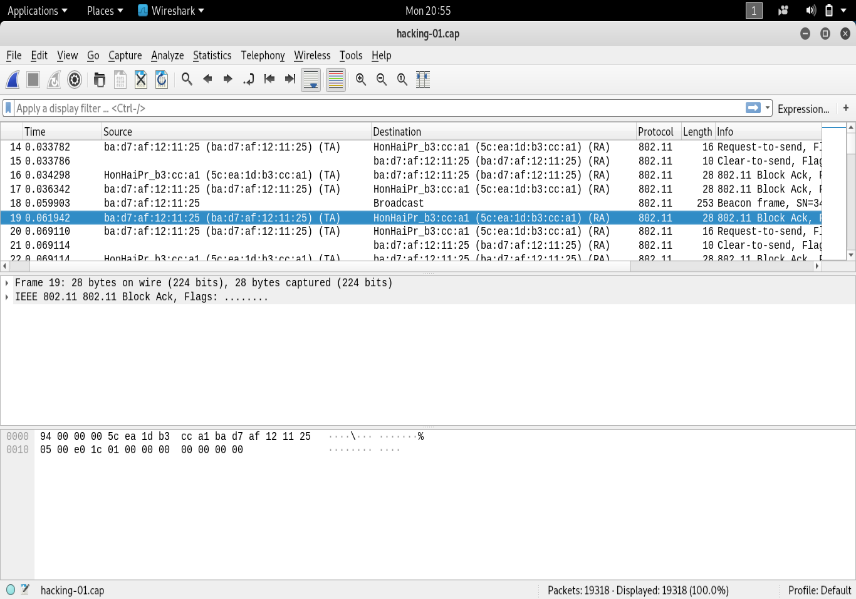


Figure 3: MAC address of device to be disconnected

We will now open the saved file using Wireshark in order to identify the brand of device we try to disconnect and then we can see the mac address of the device which we want to disconnect from the network.

Wireshark is an application in kali Linux through which we can analyze packets (containing data) and enables the user to interactively browse the data traffic on a computer network.

4. Now we will apply the following command to initialize the de-authentication attack

Aireplay-ng –deauth 100000[no. of deauth requests] -a[mac address of target network](android ap) -c[mac address of victim] wlan0

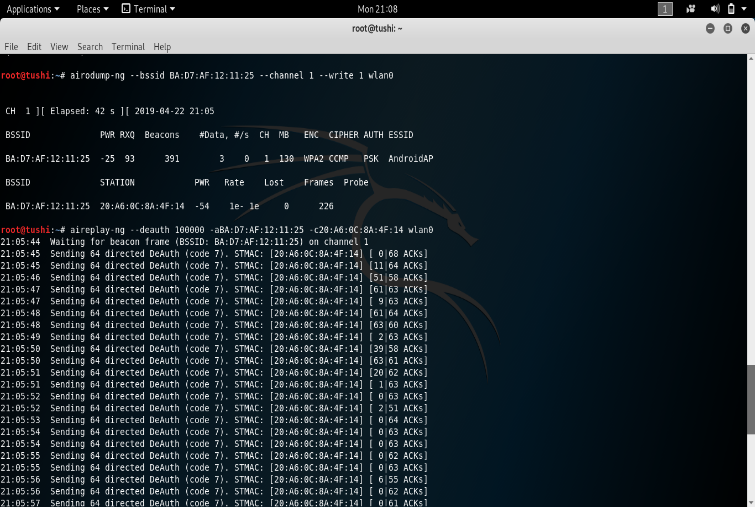


Figure 4: DE authentication attack in action

Now the device which we wanted to disconnect is disconnected hence the DE authentication attack is completed, but it can still further be used to do many other attacks like phishing etc.

**Worst nation for safety of on the internet**

This graph tells us about the worst countries in terms of safety over internet. India ranks 15th over here which is not a thing to be proud of as it is in the list of such countries where security breaches are a regular routine.

Figure 5. ranking of different countries in terms of cyber security over internet [2]

Figure 6. tells us about the nations suffering from malwares over their computers. In the year 2017 Indian government launched anti malware tools for people to use but clearly it is signified that it didn’t work as 22% people are still facing serious threats over the large devices.

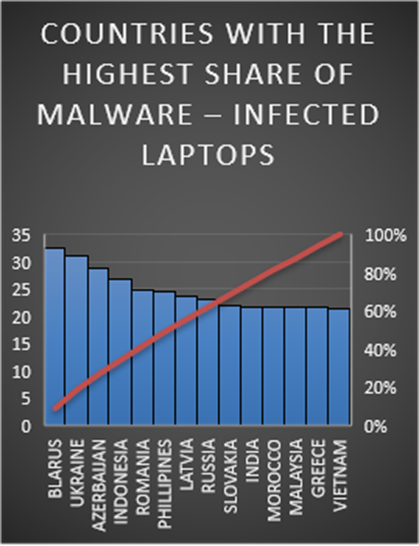


Figure 6: Countries with highest no. of laptop infected with malwares [2]

The figure 7. tells us about the nations in which many mobile phones are infected by malwares the problem of these nations is that they are overpopulated hence offering a large market for hackers. They use cheap tools to protect their devices hence suffer from infected phones

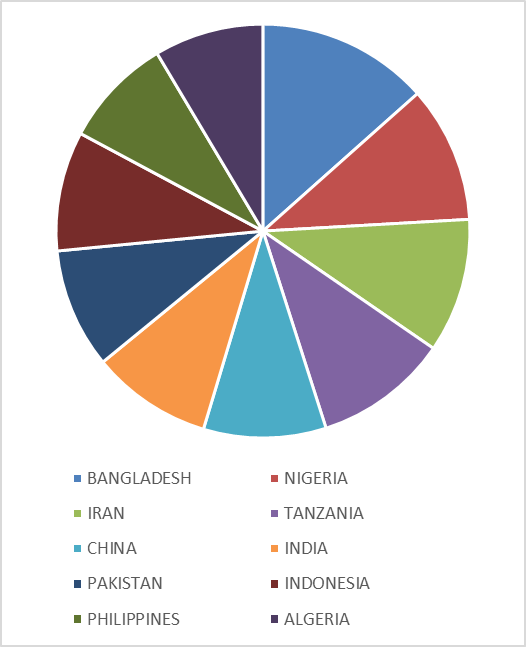


Figure 7: Countries with highest no. of mobile phones infected with malwares [3]

**VIII. CONCLUSION**

In this paper we discussed about the adversity which multinational companies face from black hat hackers, also we enlighten the readers about India’ s current situation around the world in terms of security. India is lagging in security due to lack of knowledge discussion about a simple de- authentication attack has also been included in this paper which is vital for cracking WPA or WPA2 security.

**References**

1. <https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks>
2. <https://qz.com/india/1544739/india-ranks-among-the-worst-in-the-world-for-cybersecurity/>
3. <https://www.theatlas.com/i/atlas_B1MxmEFEV.png>
4. M. Lehrfeld and P. Guest, "Building an ethical hacking site for learning and student engagement," SoutheastCon 2016, Norfolk, VA, 2016, pp. 1-6, doi: 10.1109/SECON.2016.7506746.
5. Rathore. N (2016). Ethical Hacking and Security Against Cyber Crime. *i-manager’s Journal on Information Technology*, 5(1), 7-11.
6. Georg, Thomas, Burmeister Oliver, and Low Gregory. "Issues of Implied Trust in Ethical Hacking." *The ORBIT Journal* 2.1 (2018): 1-19.
7. Warren, M., Leitch, S. Hacker Taggers: A new type of hackers. *Inf Syst Front* **12,**425–431 (2010). <https://doi.org/10.1007/s10796-009-9203-y>
8. Y. Wang and J. Yang, "Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool," 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, 2017, pp. 110-113, doi: 10.1109/WAINA.2017.39.
9. Brijesh Kumar Pandey, Singh, A., & Lovely Lakhmani Balani. (2015). ETHICAL HACKING (Tools, Techniques and Approaches). *Unpublished*. <https://doi.org/10.13140/2.1.4542.2884>
10. <https://www.gdatasoftware.com/blog/2018/09/31037-malware-figures-first-half-2018-danger-web>.
11. Chibiao Liu. 802.11 Disassociation Denial of Service (DoS) attacks: [www.mnlab.cs.depaul.edu/seminar/spr2005](http://www.mnlab.cs.depaul.edu/seminar/spr2005)
12. Aslam, Baber, M. Hasan Islam, and Shoab A. Khan. “802.11 disassociation DoS attack and its solutions: A survey.” Mobile Computing and Wireless Communication International Conference, 2006. MCWC 2006. Proceedings of the First. IEEE, 2006
13. Sharma, Shweta, and Meenakshi Mittal. “Detection and prevention of de-authentication attack in real-time scenario.” (2019).
14. Bahaweres, R. B., S. Mokoginta, and M. Alaydrus. “Comparison of methods for localizing the source position of deauthentication attacks on WAP 802.11 n using Chanalyzer and Wi-Spy 2.4 x.” *Journal of Physics: Conference Series*. Vol. 801. No. 1. 2017.
15. Rathore, Neeraj Kumar. "Ethical hacking & security against cyber crime." *Journal on Information Technology (JIT)* 5.1 (2016): 7-11.
16. M. Lehrfeld and P. Guest, "Building an ethical hacking site for learning and student engagement," SoutheastCon 2016, Norfolk, VA, 2016, pp. 1-6, doi: 10.1109/SECON.2016.7506746.
17. Z. Trabelsi and W. Ibrahim, "Teaching ethical hacking in information security curriculum: A case study," 2013 IEEE Global Engineering Education Conference (EDUCON), Berlin, 2013, pp. 130-137, doi: 10.1109/EduCon.2013.6530097.