Ethical Hacking: Cyber-Crime Survival in the Digital World

C Nagadeepa, Reenu Mohan, Ajeet Singh Shekhawat

***Abstract*: An ethical hacker is a person or a company who has permission from the owner of the system or network to test and penetrate the system in order to find any kind of vulnerabilities, weaknesses or loopholes in the network so that these can fixed and system can be secured from black hat hackers. Ethical hackers use the same kind of tools and methods to test the system as black hat hackers. As we are in digital world it is necessary to protect our network from various hacking attack on our networks. If we have our networks tested and secured, we can protect our data and digital footprints from going into wrong hands.**

Current research paper will talk about the most common kind of hacking attack by black hat hacker "network hacking" just by gaining access to the AP of your network and simply putting some commands and all your data can be captured and altered through some software provided by the platform like kali Linux.

To safeguard our data, among the various technologies are WEP, WAP and WAP2 are used prominently. Which also have some vulnerability in it, this research paper will be discussing about these weaknesses of each technology in detail and at last it will also be discussed on different ways to protect our mobile, system, etc from such attempts of hacking into our networks.

***Keywords*: Hacking, Ethical hacking, network hacking, WEP,WAP,WAP2,AP**

I. INTRODUCTION

A. *Cyber-crime survival in the digital world*

Ethical hacking is the branch of computers which check the security of a system and network. The main job of ethical hackers is to secure the data from black hat hackers, ethical hackers use the same methods as used by black hat but they have permission from the network administrator for doing so. It is very important that we secure our data in this growing digital world where even our biometric signatures are also digitalised. Just imagine being your biometric and other data stolen by a hacker, and the ways in which he can use it to harm you financially, mentally, etc. various companies pay millions to such ethical hackers. It is a matter of fact that even after paying so much companies are losing billions every year due to such hacking activities.

Current research paper will talk about the role of ethical hackers in the cyber world and the ways in which our information stored in our devices is hacked by the black hat hackers as well as the precautions that can be taken to secure our data and information from hackers. In here we will be talking about the most successful and reliable attack of hackers which has a very high success rate as compared to others "Network Hacking". The main aspects of network hacking are WEP, WAP, WAP2, WPS. We will be discussing about these aspects of network hacking in much detail in the current research paper.

Manuscript published on November 30, 2019.
* Correspondence Author

Dr. C. Nagadeepa*, Assistant Professor, Department of Commerce, Kristu Jayanti College, Bangalore, India. Email: cnagadeepa@gmail.com
Dr. Reenu Mohan, Assistant Professor, Department of Commerce, Kristu Jayanti College, Bangalore, India. Email:reenu@kristujayanti.com
Ajith Singh, IV B.Com, Department of Commerce, Kritu Jayanti College, Bangalore, India.

B. *Objectives of ethical hacking :*

- To secure the network from any hacking attacks.
- Finding any kind of vulnerability in the network and check whether it can be used to harm the owner or not.
- To counter any live/ongoing attack of hackers on the network and system.
- To protect the stored data with the help of various kinds of encryption techniques.
- It also helps in protecting various kinds of biometric signature.

II. LITERATURE REVIEW

A recent ethical hacking research papers issued by various people only talked about the methods used by black hat hackers after getting access to the system. But this research papers will be discussing about the way a black hat gets an access in networks and systems and the ways we can protect ourselves from such an attack.

According to my research a black hat hacker can attack you only if he breaks into your system or network. As the famous line goes "precaution is better than cure"

III. OBJECTIVE OF THE STUDY

- To know various aspects of network hacking.
- Various encryption used by us to protect our data on a network.
- Flows of such encryption.
- How to protect our data by eliminating such disadvantages of such technologies

IV. DISCUSSION

A. *Ethical Hacking*

Ethical hacking is a hacking done with the aim of protecting ones data, system and network from malware, virus, black hat hacker, etc. Ethical hackers are people with proper knowledge of various methods to protect the data, information,etc. from black hat . Ethical hackers use the same methods to pen test the systems and find vulnerabilities in them so that they can be fixed and black hat hackers cannot use them to enter the network.

Ethical hackers have permission of hacking the system from the owner or administrator.

In the recent year data which is being termed as the new gold of this digital era. Hence, no company would like to get the data of their customers to be hacked so they hire ethical hacker for the job of protecting the data from hackers at the cost of millions of dollars each year. New companies have been made for the specialised work of protecting the data called **Cyber security companies.**

Every year not just companies but various governments are on the target of black hat hackers to obtain sensitive and classified information from various departments of the government. There are many instances of hacking in the past but as we are moving forward on the timeline, these hacks are getting lethal with each passing day.Hence there is a growing demand for ethical hackers in the new world.

For instance the recent attacks on a nuclear plant (Kudankulam nuclear power plant) ,though there was no significant loss but such hacks have raised a question on the security of such nuclear plants ,hacking a popular social media app whatsapp which resulted in leak of account data of around 1,400 people in may 2019.

Ethical/black hat hackers use various methods of hacking such as DoS(denial of service) attack, network hacking, malware, phishing, etc. In the current research paper we will be talking about network hacking in detail. We will be looking at the various techniques used to protect our data and the flows of such techniques used by hackers to hack into our system. This research paper will further discuss about the measures which can be taken to overcome the flows of such technologies.

Network hacking is among the most reliable methods of hacking a system because there are some techniques which do not let the user know that their system is being hacked and still the sensitive information goes into the hands of hackers. To deal with the problems of network hacking the technologies used to transfer information from one user to another has been developing. Let us see various technologies and their merits ,demerits and the ways to overcome their flows/error.

B. *WEP(wired equivalent privacy)*

It is the oldest encryption used to transmit data from one user to another. Though it is very useful as compared to an open network.it is still being used by some network. It uses an algorithm called RC4 for encryption, but still it is very easy to crack it. Let us first see how we actually transfer data from one system to another :

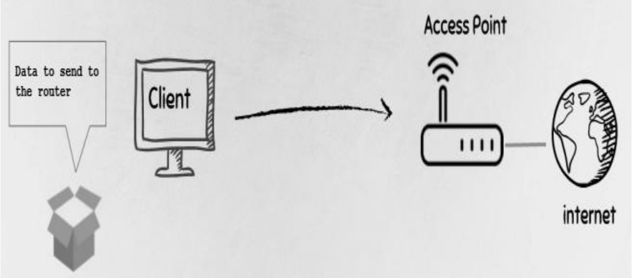

Fig1: wired equivalent privacy

Same basic is used in the encryption is used in WEP, WAP and WAP2

Steps of getting information from the internet are :

Step-1 : So what happens in this is that first a user packs /encrypts.

Step-2 : After encryption we send the packet to the **AP**(access point)/ router.

Step-3 : Then the processed result is sent back to the client back the same way with the help of packets.

The point which we should focus here is that the way an access point decrypts a packet encrypted by WEP, which uses a 24 bit encryption for transferring data. 24 character bit is also called an **I.V(Initial Vector).**

So an access point uses a keystream for decryption process and a keystream is a combination of initial vector and the password for the access point.

Keystream = Initial Vector(I.V) + key(Password)

Merits of WEP(wired equivalent privacy **)**

- It helps in protecting our data from hackers in a better way as compared to an open system.
- A good level of knowledge is required in encryption and decryption, hence not everyone can crack into systems.

Demerits of WEP(wired equivalent privacy **)**

- This is a very old way of encryption of data and information.
- The encryption bit is just 24 bits only, which can be easily be cracked in a few seconds.

*Ways to overcome its WEP(wired equivalent privacy***)**

- Use better encryption such as WAP and WAP2.
- Uses a higher level of encryption such as 32,64,128 bit for encrypting the data and information.

*WPS(wi-fi protected setup***)**

Wi-fi protected setup is used for making a home or office network faster and easier to get connected to it. But this can be a drawback for you if you have not enabled Push back button (**PBB).**

By default the companies which make access point use 12345670 as a default password which can be changed by the user by going in the admin portal of your router. Hence if you have not changed the password and you have not enabled PBB, then you might get hacked very easily.

But if a user has enabled push back button(PBB) then it can be used as an enhancement to the network. It declines the access of an intruder if the PBB is not pressed before connecting with the password.

We can overcome the flow/drawback of WPS only by enabling the PBB and by changing our WPS password only.

As we are moving towards a totally digitalised world we need to take care of our data and information by yourself because not everyone cannot hire an ethical hacker for them.

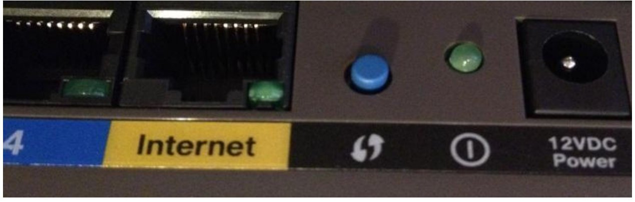

Fig2: WPS

The blue color button is a WPS button here in the above image .

*WAP and WAP2(wireless application protocol and wireless application protocol 2***)**

WAP was introduced in so that we can overcome the drawbacks/flows in WEP(wired equivalent protection). And later on the next version with a better encryption of data was introduced called WAP2. It had an encryption of 128 bit which makes it too hard to crack easily but still it can be.

Packets encrypted by WAP does not contain any information which can be used black hat hackers to crack the password to system or network. The only possible way of cracking the password of such networks is to capture the **handshake.**

Handshake refers to the packet where a user connects to the access point using a password and this is the only way of cracking the password.

But a black hat hacker would not wait for you or anyone else to connect to the network and getting the handshake between the user and the access point. Hence black hat users use attacks such as :

1. DE authentication attack
2. Fake Authentication attack

What basically these attacks do is that they disconnect the user from the access point for a very short duration about which he might not even notice maybe just for a second or longer. Since we know that once we get disconnected from the network we need to associate with the network once more using the password, hence this way the black hat hacker gets the handshake required for the process of cracking the password.

Once a black hat hacker gets the required handshake he uses a technique called brute forcing the password, where in we use various various combinations of alphabet, numbers, and symbols for guessing the password and checks each generated password for connecting to the access point or network.

The method which we discussed above takes a whole lot of time hence black hat hackers does not prefer doing it as it requires more powerful systems for processing the generated passwords and all .

Another and a little easier way of cracking the password is cracking the password using a particular word list . so wordlist is a collection of various combinations of letters and numbers as well as symbols. We can generate wordlist as per are requirements through various wordlist generator or we can can get such word list from the internet but **it is illegal to do so.**

In this era of digitalisation we need to be careful of such attacks and now let's see what is the difference between WAP and WAP2.

WAP use the TKIP(terminal key integrity protocol) algorithm for encryption whereas WAP2 is capable of using TKIP as well as a more advanced algorithm for encryption called AES(advanced encryption standard).

The bit used by WPA for encryption is just 64 bits whereas the bits used by WAP2 for encryption is 128 bits. So after seeing the difference between the WAP and WAP2 it is highly recommended to use WAP2 for network security and for home use as it is considered to be very hard to crack the password of such networks.

Merits of WAP and WAP2 (wireless application protocol)

- Both the encryption methods are much more secure and better as compared with the WEP(wired equivalent protection).
- It is not at all easy for anyone to crack the password for WAP and WAP2.
- These encryption techniques does not have any flows in them as WEP.
- WAP2 is better than wap as it uses a 128 bits encryption whereas wap use only a 64 bit encryption.

Hence it is advised if you want your data to be secured than use WAP2 for network and systems.

Demerit of WAP/WAP2 **:**

- It has only one flaw that access point which was designed and manufactures earlier then WPA2 method require too much power to protect your data.

Some tips and tricks to protect your system and network are:

- Never use the same password everywhere .
- Make sure that your password is a combination of alphabets, numbers and symbols.
- Use a password that is difficult to guess.
- Change your password on a frequent basis.
- Always use a network with WAP2 encryption.
- Try not to use public hotspot for internet usage.

V. CONCLUSION

We have discussed all techniques used for encryption of data as well as discussed various ways in which black hat hackers hack your network. We have seen various flaws of all such techniques.

For each one of us, data which is being transmitted on a network is crucial and hence we should try our best to protect it from going in the wrong hands. Moreover stolen data is truly a bag of gold for black hat hacker. It may be a file with some random letters for a normal person but for them it is very resourceful. They can use this data against you or they may sell it to others for earning some bucks etc

REFERENCES

1. www.ethicalhacking.com
2. www.eccouncial.org/ethical hacking
3. www.cyberlawportal.com
4. www.cisecurity.org
5. Ashish Pandey : Cyber Crimes Detention and Prevention.
6. Apurba Kumar Roy : Role of Cyber Law and its usefulness in Indian IT Industry
7. Charles P. Pfleeger : Security in Computing.
8. Edward Amorso : Fundamentals of Computer Security Technology

AUTHORS PROFILE

First Author: Dr.C. Nagadeepa, M.Com, M.B.A, P.G.D.C.A, Ph.D, working as Assistant Professor in Department of Commerce, Krstu Jayanti College, Bangalore - 56. She has more than 20 years of experience in teaching. She is expertise in accounts, Income Tax and Marketing subjects and having ample knowledge in computer. She has published more than 25 articles in National and International Journals. She has participated and presented papers at National and International Conferences also. She is interested in research related to e-commerce, marketing and accounts. She is guiding many students in the field of Human Resource Management, Marketing, Finance and Accounts in various universities.

Second Author Dr.Reenu MohanMBA,PGDRM,PGDLL,Ph.D Working as Assistant professor with the Department of Commerce,Kristu Jayanti College,and Bangalore.She has been teaching MBA, BHM and B.Com students for more than five years.She has presented several papers in national conferences and published articles on Competency models, Employee welfare and Talent management practices.

Third Author: Ajeet Singh Shekhawat has completed his class 10th and 12th from Army public school, Bikaner and is currently pursuing his B. COM (ACCA) from Kristu Jayanti College, Bangalore - 56. He has an interest in computers and likes to learn more and more about technology. He has received best paper award in national conference held in Surana College. He actively participates in various research activities conducted by inter and intra college fests.

Retrieval Number: D4612118419/2019©BEIESP
DOI:10.35940/ijrte.D4612.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication