ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 4 April 2017, Page No. 21042-21050
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.42

Ethical Hacking and Hacking Attacks

Aman Gupta, Abhineet Anand
Student, School of Computer Science and Engineering, Galgotias University,Greater Noida, India
amang9578@gmail.com
Professor, Department of Computer Science and Engineering, Galgotias University,Greater Noida, India
Abhineet.mnnit@gmail.com

Abstract: -

As nowadays all the information is available online, a large number of users are accessing it, some of them use this information for gaining knowledge and some use it to know how to use this information to destroy or steal the data of websites or databases without the knowledge of the owner. The purpose of this paper is to tell what is hacking, who are hackers, what is ethical hacking, what is the code of conduct of ethical hackers and the need of them. A small introduction of Linux Operating System is given in this paper. All the techniques are performed on the Linux operating system named Kali Linux. After this some basic hacking attacks covered in the paper are MiTM Attack (Man in The Middle Attack), Phishing Attack, DoS Attack (Denial of Services Attack). Further what is Wi-Fi, what are the techniques used in the Wi-Fi protection and the methods used by the hackers to hacks Wi-Fi passwords is covered in the paper.

Keywords: -Hackers, Ethical Hackers, MiTM, DoS, Phishing, Wi-Fi phishing, Code of conduct.

Introduction: -

As the computer technology advances, it has its darker side also; HACKERS. In today world the size of the internet is growing at a very fast rate, a large amount of data is moving online, therefore, data security is the major issue. The internet has led to the increase in the digitization of various processes like banking, online transaction, online money transfer, online sending and receiving of various forms of data, thus increasing the risk of the data security. Nowadays a large number of companies, organizations, banks, and websites are targeted by the various types of hacking attacks by the hackers. Generally, after hearing the term hacker we all think of the bad guys who are computers experts with bad intensions, who tries to steal, leak or destroy someone's confidential or valuable data without their knowledge. They are the persons with very high computer skills who tries to break into someone else security for gaining access to their personal information, but all the times it is not like that. To overcome the risk of being hacked by the hackers we have Ethical Hackers in the industry, who are also computer experts just like the hackers but with good intensions or bounded by some set of rule and regulations by the various organizations. These are the persons who try to protect the online moving data by the various attacks of the hackers and keeping it safe with the owner. Further, this paper tells you more about hackers, ethical hackers and Linux operating system (kali Linux) and aware you about some attacks performed by the hackers on the internet.

What Is Hacking?

Hacking is the technique of finding the weak links or loopholes in the computer systems or the networks and exploiting it to gain unauthorized access to data or to change the features of the target computer systems or the networks. Hacking describes the modification in the computer hardware, software or the networks to accomplish certain goals which are not aligned with the user goals. In contrast, it is also called breaking into

someone's security and stealing their personal or secret data such as phone numbers, credit card details, addresses, online banking passwords etc.

Hackers: -

The term HACKER in popular media is used to describe someone who breaks in to someone else's security using bugs and exploits or use his expert knowledge to act productively or maliciously. Hackers are the computer experts in both hardware as well as software. A hacker is a computer enthusiast and master in a programming language, security, and networks. He is kind of person who loves to learn various technologies, details of the computer system and enhances his capability and skills. According to the way of working or based on their intensions HACKERS can be classified into three groups

1. White Hat Hackers

2. Black Hat Hackers

3. Grey Hat Hackers

1. White Hat Hackers: -

A white hat hacker is a computer security specialist that breaks into and find loopholes in the protected networks or the computer systems of some organization or company and corrects them to improve the security. White Hat Hackers use their skills and knowledge to protect the organization before malicious or bad hackers find it and make any harm to the company or the organization. White Hat Hackers are the authorized persons in the industry, although the methods used by them are similar to those of bad hackers but they have permission from the organization or the company who hires them to do so.

2. Black Hat Hackers: -

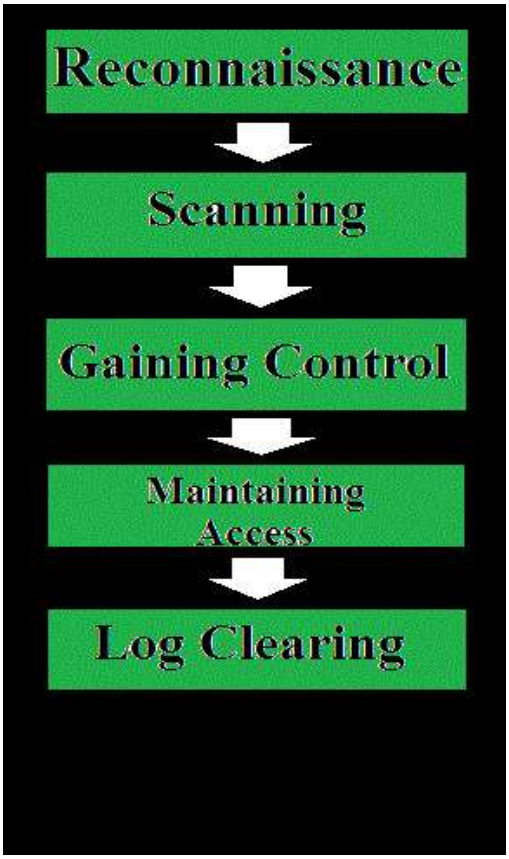
A Black Hat Hacker also known as a "Cracker" is a computer hardware and software expert who breaks into the security of someone with malicious intent or bad intentions of stealing or damaging their important or secret information, compromising the security of big organizations, shutting down or altering functions of websites and networks. They violate the computer security for their personal gain. These are persons who typically wants proves their extensive knowledge in the computers and commits various cybercrimes like identity stealing, credit card fraud etc.

3.Grey Hat Hackers: -

A Grey Hat Hacker is a computer hacker or security expert who sometimes violates the laws but does not have any malicious intentions like the black hat hackers. The term Grey Hat is derived from the Black Hat and the White Hat as the white hat hackers finds the vulnerabilities in the computer system or the networks and does not tells anybody until it is being fixed, while on the other hand the black hat hackers illegally exploits the computer system or network to find vulnerabilities and tells others how to do so whereas the grey hat hacker neither illegally exploits it nor tells anybody how to do so. Grey Hat Hackers represents between the white hat hackers who operate to maintain system security and the black hat hackers who operate maliciously to exploits computer systems.

Now the methodology or the path followed by the Hackers is as follows: -

DOI: 10.18535/ijecs/v6i4.42



Reconnaissance: -

The process of collecting information about the target system is called reconnaissance. The process includes finding vulnerabilities in the computer system, which means finding the ways which are left vulnerable. The further process of hacking is carried by the hacker if the hacker finds any way to access the system. At the end of the reconnaissance phase the hacker has a bunch of information using which he can construct a promising attack on the target system.

Scanning: -

Before the attack hacker wants to know what system is up, what applications are used, what are versions of the applications. In scanning, searching of all open, as well as closed ports, is done means finding a way to enter the system. It includes obtaining target's IP address, user accounts etc. In this phase the information gathered in the reconnaissance phase is used to examine the network and tools like Dialers, Port scanners etc. are used. Nmap is the popular, powerful and freely available tools used in scanning.

Gaining Controll: -

This is the real part of the hacking procedure where the information gathered in the previous two phases is used to enter and take control of the target system through the network or physically. This phase is also called "Owning the System".

Maintaining Access: -

After gaining entry in the system in the previous step the hacker maintains the access to system for the future attacks and make changes in the system in such a way that any other security personal or any other hacker does not get the entry into the system into which is hacked. This is the situation in which the attacked system is known as the "Zombie System".

Log Clearing: - It is the technique of removing any leftover log files or any other types of evidences on the hacked system from which the hacker can be caught. There are various tools in the ethical hacking techniques from which a hacker can be caught like penetration testing.

After reading about hacking and the shades of hackers there should be some way or some technique of protecting the computer system or the computer networks form the malicious hackers, therefore the terms "Ethical Hacking" and "Ethical Hackers" came into the industry.

Ethical Hacking: -Ethical hacking is a branch of information security. It is also called "Penetration Testing" or "White Hat Hacking". It is a type of hacking performed by an individual or a company, which helps in finding threats and loopholes in the computer system or network's security of the organisation. The techniques or the methods used in the ethical hacking are very similar to those of malicious hacking but the difference is they are legal here they are used in a productive manner. The information gained from ethical hacking is used in maintaining system security and to prevent the system from any further potential attacks.

Ethical Hackers: -The White Hat Hackers are called the "Ethical Hackers". They are the paid professionals. As told earlier they are the computer experts who hack the computer system or network earlier and correct or fix all the security issues in the system or network before they are being noticed by the bad hackers who tries to break in or act maliciously.

The Code Of Conduct Of An Ethical Hacker: -

- Identifying and determining the confidentiality and privacy of the data of any organisation before hacking and should not violate any rule and regulations.
- Before and after the hacking maintaining the transparency with the client or owner of the organisation.
- The intensions of an ethical hacker must be very clear, that not to harm the client or organisation.
- Working within the limits set by the client or the organisation, do not go beyond them.
- After the hacking do not disclose the private or confidential findings during the hacking with others.

Need Of Ethical Hackers In The Industry: - As every organisation has its own confidential information which can be hacked by the malicious hackers or can be damaged by them therefore in order to protect that information the organisations heir ethical hackers and allow them to hack their own systems ethically any find flaws or loopholes in their systems and correct them before any hacker hacks it.

Now starting with some hacking attacks performed by the hackers over the internet. Before that there is need of knowing Linux operating systems and what are their use in performing hacking attacks.

Linux Operating Systems: -As the name tells it is an operating system just like the windows and Mac. An operating system is an interface between the user and the computer hardware, it manages all the hardware resources available with the computer. In the computer system an OS is required for working of various applications.

Unlike Microsoft Windows and Mac operating systems the Linux are the open source operating systems as it is distributed under open source license. It is more secure than the windows and has very less number of viruses known which will harm Linux OS. Some of the Linux operating systems are Ubuntu, Kali Linux, Fedora, Linux Mint etc.

Further in this paper the attacks are performed on the Kali Linux Operating System. Kali Linux Operating system is a Linux distribution which is mainly used for penetration testing and security auditing. Kali Linux contains various tools for computer forensics, penetration testing, reverse engineering etc. Kali Linux is developed by "Offensive Security".

Now starting with the Phishing Attack: -

For performing all these attacks kali Linux must be installed on the system.

Phishing: - Phishing is a cyber-attack or say an online fraud in which the hacker attempts to gain some private or secret information from the victim like password, login information, credit card numbers, email ids, online banking pin numbers etc. It is done by sending fake emails or creating fake websites which looks very similar to the original ones.

Steps for performing phishing on Kali Linux: -

1. Open the terminal in kali Linux and type **setoolkit** and press enter.
2. After that press **y** and enter.
3. Now select **1. Social Engineering Attacks**.
4. After that select the second **2. website attack vectors** and enter.
5. Now select the **3. credential harvester attack method**.
6. After this select second**2. site cloner**.
7. Now the command is asking for the IP address, for this open a new terminal window and type **ifconfig** and from their copy the **inet address** and paste in the previous window and press enter.
8. After this type the address of the website which you want to clone and press enter. It will take some time to clone the website
9. After the process completes open the new terminal window and go to www directory using command **cd /var/www**.
10. After going to this directory enter **ls** in the command line and press enter. There you will a file similar to this Harvester_2016-01-01 10:37:25.332885.txt after that enter this command in the terminal window **cat Harvester_2017-03-20\ 10\:37\:25.332885.txt**
11. After entering the previous command, the email id and password of the victim who enters on the fake or copied website will be shown.

All these steps work on the local computer system or the devices connected with LAN to your computer system and Apache2 server must be configured.

Now the second hacking attack is the DoS (Denial of Services) Attack: -

Denial of Services(DoS): -It is a type of cyberattack in which the attacker's aim is to make a machine, website or a network resource unavailable for its end users temporarily or for an indefinite time period and disrupting the services of a host connected to the internet. This attack is basically done by flooding the target website, server or the machine with a very large number of requests and making it overloaded, therefore the target is unable to fullfill most or all of the requests. The DoS attacks can last for days, weeks or even for months. The attacker's speed of sending requests to the target server or the website is very fast in several hundred of mbps or gbps.

DOI: 10.18535/ijecs/v6i4.42

Steps for performing a Dos attack on Kali Linux: -

1. Open the terminal in kali Linux and type the command **hping3 –c 100000 –d 120 –S –w 64 –p 21 –flood –rand-source (address of the target website)** and press enter.

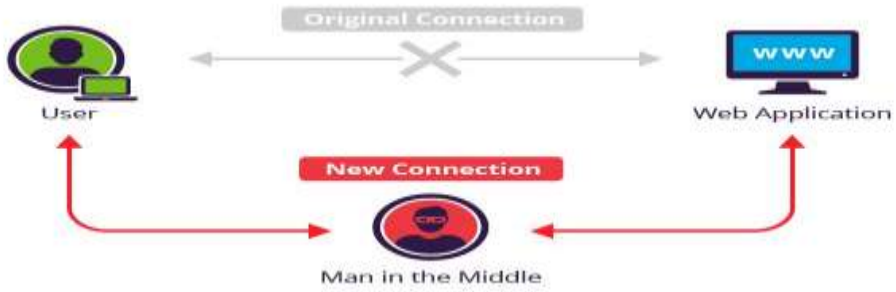
   In the above command meaning of different parameters are as follows:-
   hpin3 is the name of the application binary.

   –c 100000 is the number of packets to send.
   –d 120 is the size of each packet that is to be sent to target machine.
   –s means sending SYN packets only.
   –w 64 means the TCP window size.
   –p 21 is the destination port (21 being FTP port). You can use any port here.
   –flood means sending packets as fast as possible, without taking care to show incoming replies.
   –rand-source means using Random Source IP Addresses.
2. After entering the previous the DoS attack is started to see how the attack is working open a new terminal and type **tshark** and press enter there you will be able to see how packets are sent to the target.
3. Now to stop the attack press **ctrl+c** in the DoS attack terminal window. After that you will be able to see how many packets are sent.

This is only a tutorial therefore this will not shut down and website or any server as for that the request or the packet sending speed must be very high as discussed above and nowadays any modern firewall can block this type of attacks.

Now the third hacking attack is the Man in the Middle(MiTM) attack: -

Man in The Middle Attack: - The man in the middle attack is the attack in which the attacker tries to enter in between the conversation of the two parties or two devices and can access all the information sent and received by them. In this attack, the sender and the receiver think that they are connected through the original connection but it is not that as the attacker makes an independent connection with both the victims, can access the information in the middle, and can alter it. Here the MiTM attack is covered in kali Linux using Ettercap Tool.



Steps for performing a MiTM attack on Kali Linux: -

1. Open the terminal and type the command **echo 1 >> /proc/sys/net/ipv4/ip_forward** and press enter.
2. After that enter the command **leafpad /etc/Ettercap/Ettercap.conf** and press enter, a window will open and in this window you will find

   ec_uid = 65534 #nobody is the default
   ec_gid = 65534 #nobody is the default

   here replace the number **65534** and replace it with **0** in both the lines. After that click on the **Search** option in the toolbar and click on **Find** option.
3. In the **Find** column search **iptables.** After the search result you will see these two lines
   #redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
   #redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport".
4. Now uncomment both the lines by removing the **#** symbol and close the leafpad file and click on **save changes**.
5. Now in the terminal window enter **ettercap –G** and press enter. The Ettercap tools will start.
6. In the Ettercap tool click on the **Sniff** option then **Unified sniffing** then a dialogue box will in that select **eth0** and click on ok.
7. After that click on **Hosts** option then on **Scan for hosts** their you will see the list of host devices connected and their IP addresses.
8. After that click on the IP address of the router and click on **Add to target 1** then click on the IP address of the victim and click on **Add to target 2**.
9. Now click on the **Mitm** option in the tool bar and click on **Arp Poisoning**. After that a dialogue box will open and click on the **Sniff remote connections** and click on ok.
10. After that go to start option and click on **start sniffing**. Here you have successfully started the MiTM attack.
11. For viewing the victims url activities in the new terminal window enter the command **driftnet –I eth0**, a **driftnet** window will open where you can see the images of the websites visited by the victim.
12. To stop the MiTM attack click on the **Mitm** option and then click on **Stop mitm attack(s)**.

Wi-Fi: - Wi-Fi stands for Wireless Fidelity. It is a technology, which uses radio waves to provide wireless network connectivity to various devices available within its range. The range of Wi-Fi depends on the Wi-Fi routers. Generally, it is said the range of Wi-Fi ranges between 46m (indoor) to 92m (outdoor).

Now the three main techniques used for Wi-Fi protection are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2 (Wi-Fi Protected Access 2). The WEP is the most used technique in protecting Wi-Fi, nowadays it is not used in protecting Wi-Fi because it is very weak security standard. The passwords used in that can easily be hacked by a computer system. That is why now WPA and WPA2 security protocols are used, in this it uses a 256 bit encryption key for protection.

Methods used by hackers to hack Wi-Fi routers: -

Earlier the hackers use various methods for hacking Wi-Fi password like dictionary attack in which a very large file is prepared containing possible password or combination of several letters, numbers and special characters and use this file to hack the Wi-Fi password by selecting each combination from the file and

putting it in the password field, all this is done by computer software and consumes very much time and the success rate is very less.

The other attack used by hackers is the brute force attack in which all possible characters in upper case and in lower case and all the numbers are given to the computer and the computer system itself makes various combination and put them in the password field and tries to gain the password, but this attack is very slow and it fails in the case of special characters.

Therefore, nowadays hackers use a completely new method of hacking Wi-Fi passwords known as Wi-Fi Phishing. This technique works for hacking the password of any Wi-Fi encrypting security. In this technique the hacker blocks the Wi-Fi connection from the original Wi-Fi router and creates a evil twin or a Wi-Fi hotspot with the same name, and when the user again tries to connect to the Wi-Fi it connects to the fake one and then a page prompts on the user screen saying that some updates are made in the security and asks to enter the password. As the user enters the password, it directly goes to the hacker.

Steps for performing Wi-Fi Phishing: -

1. Open terminal in kali Linux and download Wi-Fi phisher module using command **git clone https://github.com/sophron/wifiphisher.git**.
2. Go to Wi-Fi phisher directory using **cd wifiphisher-.1.1 command**.
3. Now run the Wi-Fi phishing script using the command **python wifiphisher.py**. After that it will show **hostpad** not installed and ask to install or not here press **y** and press enter. After that again enter the command **python wifiphisher.py** and press enter.
4. After the previous step is completed it will show the list of all the Wi-Fi it will discover. After getting the list press **ctrl+c**.
5. After it will ask to choose the number of AP you want to copy, here enter the corresponding number of your target Wi-Fi from the previous list and press enter. As soon as you press enter the target Wi-Fi gets attacked and cloned.
6. Now when they try to re authenticate they will be connected to the cloned Wi-Fi router and a page will prompt on their screen saying that a firmware upgrade is available enter password to upgrade. As the victim enters the password it directly appears on your terminal window.

Some of the tools used by the ethical hackers

Port Scanners	Nmap, Superscan, Angry IP Scanner, Nikto, Unicornscan, Autoscan.
Packet Sniffers	Wireshark, TCPdump, Ethercap, Dsniff, EtherApe.
Vulnerability Exploitation	Metasploit, Sqlmap, Sqlninja, Social Engineer Toolkit, Netsparker, BeEF, Dradis
Vulnerability Scanners	Nessus, OpenVAS, Nipper, Retina, QualysGuard, Nexpose.
Hacking Operating System	Backtrack5r3, Kalilinux, SE Linux, Knoppix, Backbox linux, Pentoo, Matriux, Krypton, NodeZero, Blackbuntu.
Intrusion Detection Systems	Snort, Netcap

Conclusion: - The whole world is moving towards the enhancement of technology, and more and more digitisation of the real world processes, with this the risk of security increases. This paper described the working of malicious hackers or crackers on one hand who tries to illegally break into the security and on the other hand white hat hackers or ethical hackers, who tries to maintain the security. As in the computer system, hacking plays a vital role as it deals with both sides of being good or bad. Further, this paper tells about the types, working, and various attacks performed by the hackers. In conclusion, it must be said that Ethical Hacking is a tool which when properly utilised can help in better understanding of the computer systems and improving the security techniques as well.

Refferences: -

1. Bansal, A., & Arora, M. (2012). Ethical Hacking and Social Security. Radix International Journal of Research in Social Science, 1(11), 1-16.
2. Hacking a paper by (Deepak Kumar, Ankit Agarwal, Abhishek Bhardwaj)http://www.ijcstjournal.org/volume-2/issue-6/IJCST-V2I6P2.pdf
3. Study of Ethical Hacking a paper by (Bhawana Sahare, Ankit Naik, Shashikala Khandey) http://www.ijecs.in/issue/v4-i4/68%20ijecs.pdf
4. "Hacking for Dummies" a book by Kevin Beaver, CISSP (Information Security Consultant).
5. http://www.speedguide.net/faq/what-is-the-typical-range-of-a-wireless-lan-330
6. H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.
7. Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , "Ethical Hacking " , International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010
8. System Security and Ethical Hackingwww.ijreat.org/Papers%202013/Volume1/IJREATV1I1018.pdf
9. Ethical Hacking Techniques with Penetration Testing www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit2 0140503161.pdf(by KB Chowdappa)
10. Hackers: Methods of Attack and Defense. Online. Discovery Communications.28Oct.2003 .

Authors Profile:-

AMAN GUPTA,pursuing B.TECH in computer science & engineering and specialization in cloud computing and virtualization in association with "IBM" (2nd year) in "GALGOTIAS UNIVERSITY" .

DR. ABHINEET ANAND, Assistant Professor at "GALGOTIAS UNIVERSITY" and Program chair of "IBM" courses. (Aug 2016 present),Assistant Professor at "UPES" (2012 to 2016),Director at "Rashcom Computer Education Pvt. Ltd.". (Aug 1999 to 2012). *Director at Arpan Assets and Finance Management Pvt. Ltd. Dates Employed Dec 2008 – Jul 2010*. With his 15 years of academic and administrative experience, his research includes following field of endeavor: Decision Tree, nearest neighbor method, Clustering, Rule induction, Optical Fibre Switching in Wavelength Multiplexing, Automata Theory.He has published more than 20 papers in Intentional conference, 4 Intentional Journal, 3 National Journal and 3 National Conference. He has been part 6 special session at various conferences at international level as session chair/co-chair, contributed at 6 different conferences as Technical Program Committee member. His expertise also includes reviewer at more than 10 conferences and Publication group