International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

Ethical Hacking Techniques and its Preventive Measures for Newbies

Vikas Bhaskar Vooradi [1], Lavina Jadhav[2]

[1]*Student, Dept. of Institute of Computer Science, MET College, Maharashtra, India*
[2]*Assistant Professor, Dept. of Institute of Computer Science, MET College, Maharashtra, India*

Abstract - *Nowadays, each information is valuable. Due to the widely used Internet, the state of security is deplorable. Hacking is a process in which a person tries to dig out the security loopholes for a self-profit or gratification. Some of them steal the data for their Personal use or destroy the identity of the reputed company or business for their growth in the market. This paper briefly describes the Ethical hacking, types of Hacking, Preventive measures, and all its aspects.*

Key Words: **Hacker, Cracker, Password, Preventive measure, Tools**

1. INTRODUCTION

As we know, everyone needs to be connected, and this can only be possible through the Internet. However, a little care is always must when exchanging of sensitive information with the outsider, friends, or a loved one as hacking is known for its negative impact throughout the internet era. One's Protection is always must overcome the damage associated with it - academically, professionally or emotionally.

2. THE TRUTH ABOUT HACKER'S

A hacker may be an individual or a group of People working together to break down the System in an illegal way to gain access to it. Not anyone who knows the common Computer Programming language can be a Hacker. To be a hacker, one must have in-depth knowledge about networking, software and hardware functionalities and professionally expert in Programming is considered as a Hacker.

3. WHAT IS ETHICAL HACKING?

Ethical hacking is a hands-on method performed by the authorized user. They have full access to the System where they can trace out the vulnerabilities and forward the security jerks to the higher authorities or Owners. They are known as White Hackers who work for the Organization or the companies.

4. TYPE OF HACKER'S

Fig -1: Type of Hackers

1. **White Hat Hackers**
   The well-known name for white hackers is "Ethical Hackers." They have in-depth knowledge about the Networking Protocols, Software and Hardware functionalities and professionally trained Administrators. As all rights which Admin as. They perform penetration Testing and vulnerability assessments. They work for the Organization and are well salaried. They always think at intruder point of view what an intruder can do to infect the target system to gain unauthorized access to modify the sensitive information. They follow the same procedure to see what the adverse effect is. If the outcome is Critical, they raise a report about the threat, which as posed to the Higher Authorities. Moreover, find the remedy for it.

2. **Black Hat Hackers**
   The well-known name for black hackers is Crackers." They have similar skills as that of White Hackers. However, they use their skills for the wrong purpose. Their main intention is to steal the Data with unauthorized access. They mainly target

the corporate data, violating privacy, damaging the System, and blocking the network communication channel.

3. **Gray Hat Hackers**
Gray Hat Hackers are blends of both White Hackers and Black Hackers. They do the hacking without the permission of the Owners. Their main intention is to exploit the security weakness in a system and bring issues to the attention of the Owners. They do the hacking for fun, to get an appreciation and little bounty from the Owners. They even offered a good salaried job from owners. However, they are not in search of employment.

4. **Red Hat Hackers**
They are the Blend of Both White Hackers and Black Hackers. They usually target the top level channels like Government Agencies, secret Hub, or anything that comes under the sensitive information.

5. **Blue Hat Hackers**
They are Outsiders. Who are security professionals and are Cordially invited by the reputed Companies to trace out the Vulnerabilities and Security Black holes before launching their software product to the Global market.

6. **Elite Hat Hackers**
They are really on the front edge of both the computer and network channel. The newly spotted exploits are revealed amongst these hackers first.

7. **Script Kiddie**
They are immature, non-expert, unskilled hackers. Who makes use of the pre-packaged automated tools which are developed and programmed by others to gain access to the System Usually, termed as kiddies. Who as little understanding of the underlying concept.

8. **Neophyte**
They are" Newbies." Who does not have prior knowledge about hacking? They are Unskilled like Script kiddies. However, Script Kiddies are much better than Neophyte. Neophyte needs a little time to develop their skills to compete with the Script Kiddies.

9. **Hacktivist**
They make use of Tools and Technologies to spread out the Secrets, religious or political messages to the public. These are usually done by hijacking the website and leaving the warning message on the hijacking website. The Primarily targeted sites are Government Websites.

10. **Phreaker**
They are telecom network Hackers. Who illegally makes use of Telephony system to make calls without paying for them. Their main reason is to stay as unknown. Moreover, threatened people for their personal use and get some money.

5. PHASIS OF HACKING

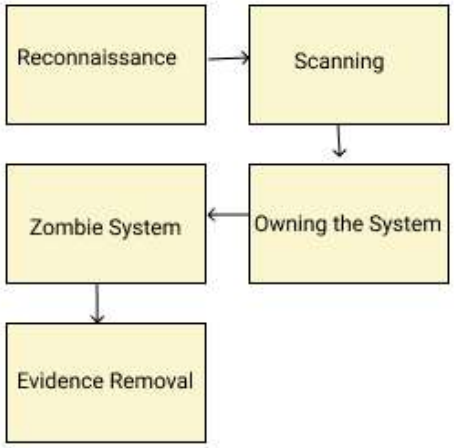

Fig -2: The process of hacking

- **Reconnaissance**
It refers to the first phase. In this phase, the attacking done in two approaches firstly passive and secondly active. In the passive phase, the attacker tries to gain information about the target system without being involved in the interaction with the target indirectly. The passive stage is also called gathering information. Most of the time, the data collected through a bribing giving to the employee working in that targeted organization who would reveal the useful information. Whereas in the active phase, the attackers try to gain access to the target system by a direct mean. At this stage, the hackers try to enter into the network to discover the individual IP address, port, host, and other services. There is a high-level risk associated with it may get caught during this active activity.

- **Scanning**
In this Scanning phase, the attacker tries to find a way to gain access to the target system by examining the network. For gaining entry in the target system, they make use of specialized tools such as diallers, port scanners, network mappers, vulnerability scanners, ping tools, and other essential tools.

- **Owing System**
  It is the real hacking phase of hackers. Whereas, by using the first two stages of information. The attacker tries to gain access to the Target system.

- **Zombie System**
  In this phase, after gaining access to the target system, the first thing the attacker does is make the system under their control by changing the system config files and privileges for future use. Even they make sure that gaining access to the system does not work at the end, they make use of the backdoor's methods to gain access. The attacker makes this secure backdoor access available for themselves at the time of changing the config and privilege by adding is own script, which could change the entire permission of the target system to bring the system under their control.

- **Evidence Removal**
  At this stage, the attacker tries to trace out all the activities performed on the victim machine. Then removes or hides all the activities. Even they overwrite the server, application, and log files to avoid the risk of getting caught.

6. OPERATING SYSTEM USED BY HACKERS

Fig -3: Os used by Hacker's

- **BackTrack**
  It is a Custom Distribution designed for security testing for all levels from newbies to experts. It as a most extensive collection of tools such as wireless hacking, server exploiting, web application assessing, social-engineering available in a single Linux distribution.

- **Kali Linux**
  It is managed and funded by Offensive Security Ltd. Kali is a Debian-derived Linux distribution Specially designed for digital forensics and penetration testing. It is one of the best operating systems of hackers.

- **Parrot-Sec forensic OS**
  It is mainly based on Debian GNU/Linux combined with the Frozen box OS and Kali Linux and used to perform all sorts of Vulnerability Assessment and Mitigation, Computer Forensics, and Surf Anonymously.

- **Cyborg Hawk Linux**
  It is a most potent, well managed Ubuntu-based Penetration Testing Distro created by the team of Ztrela Knowledge Solutions Pvt. Ltd. Specially Build for ethical hackers and cybersecurity experts who are also known as Penetration testers.

- **Back-Box**
  Back-Box is an Ubuntu-based Linux distribution. It contains more than 70 tools. It helps ethical hackers and penetration testers in security assessments. The essential advantage is that its repositories get updated at regular intervals.

- **Samurai Web Testing Framework**
  Its framework based on Ubuntu 9.04. Moreover, fully Open Source. It contains lots of Web assessment and exploitation tools. Mainly focuses on testing the security of web applications.

- **Network Security Toolkit**
  NST based on Fedora. It as 125 open source security tools. Its Main Objectives are to carry out network traffic analysis, intrusion detection, network scanning, and security patching.

- **BlackArch Linux**
  Black Arch is a Linux-based Distribution. It contains more than 1600 tools. Moreover, rated as the first option to perform Web and application-based security testing.

- **GnackTrack**
  GnackTrack is an Ubuntu-based Linux distribution, and Open source. It has a GUI based GNOME desktop with the easy user interface. Moreover, it contains various significant tools like Metaspoilt, Armitage, wa3f.

7. HACKING TECHNIQUES PERFORMED BY HACKERS

- **Bait and switch**
  In this technique, the attacker buys advertising space on the website. Than Display is own advertising with catchy words which will attract the victim to click the banner ads, after clicking the ads, the User may get directed to a page infected with malware. A popup may appear which will ask the victim to install the software. If the victim installs

the software on his working hub, then it's a cup of tea for a hacker to acquire access to the laptop/computer remotely without the permission of the User. Hacker's uses this technique to threaten them and earn money.

- **Cookie theft**
  A cookie can Store Details Such as Username, Password, Credit Card for different sites that we access. If the hacker gets access to these cookies, then he may act as an actual user to authenticate himself to gain access to the Admin Panel. This attack is also known as SideJacking or Session Hijacking. Most of the time, it happens when a Website. Do not have SSL (https) added to it. A conventional method to carry out this attack is to encourage a users IP packet to pass through the attacker's machine. By monitoring the flow of packets, an attacker may gain unauthorized access to the actual user.

- **ClickJacking**
  Another name for ClickJacking Attacks is "UI Redress." It is a way of fooling the Internet user. In this technique, the hacker hides the Actual UI(User Interface) where the victim tries to access. This behavior gets to see on Movie websites, Software Downloading websites, or torrent websites. This technique is used to redirect the user to their other webpage to get views on their website to earn dollars from ads or even may ask the user to enter the details to gain access to the downloading content. If the user fills the details, then it's a cup of tea for a hacker to steal the information.

- **Keylogger**
  It is a simple software mainly developed to capture the key sequences and strokes to a log file. This log file contains all the sensitive and non-sensitive information such as username, password, banking details, and even more. That is why most of the payment gateways or a banking website force the user to use their built-in virtual keyboard instead of a personal keyboard so that the entered details will not be captured to by keylogger. It is mainly developed for the parents to keep an eye on the child what the child is surfing on the internet when they are out of town. However, because of capturing tendency, it has been used for the illegal purpose.

- **Phishing**
  It is a technique in which the replica of the real website is designed and developed with all the functionalities. As soon as the user enters his login details, the credentials get captured at the fake server. To build trust for the user, they even display the message like the server is busy, please try again later." The actual user may think there is some technical issue with this website. Then they prefer to log in after some time. In a mean, while the hacker may use his/her credentials to access the control panel and even restrict the actual user from logging by changing the Details. This method of hacking done by encouraging the user to click on the link, they pass through messages or mail.

- **Brute Force Attack**
  It is a simple process to gain access to a web page. It tries multiple combinations of the passwords repeatedly to get in. This repeated process acts like soldiers attacking a fort; however, it is time-consuming as it needs to try all the combinations.

- **SQL injection**
  If the website has vulnerabilities in its SQL DB, hackers can quickly get access to secret information by SQL injection by deceiving the system. However, this SQL Statement can allow a hacker to access essential information on the website.

- **Eavesdropping (Passive Attacks)**
  This attack is known as MITM (Man in the Middle Attack). The hacker inserts himself as an invisible intermediary between Communication Channel to monitor the activity. They even modify the data without getting themselves detected. If Data found Useful, may also share the data among the public.

- **Fake WAP**
  The hacker creates a Fake Access Point. It is one of the more straightforward hacks and needs a simple software and wireless network. Then the hacker names their WAP as some legit name like Starbucks WiFi or with any reputed company name and starts monitoring the victim. One of the best ways to come across such type of attacks is by using a quality VPN service.

- **Virus**
  It is a little piece of code inserted in a legitimate program. They are self-replicating and are designed to poison other applications.

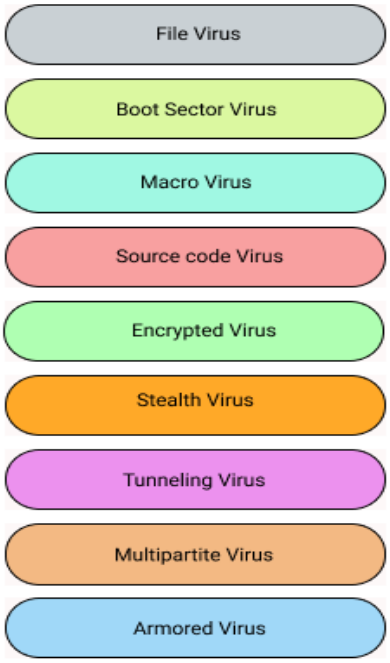

Fig -4: Types of Virus

1. **File Virus**
   This type of Virus poisons the system by appending itself to the end of the execution file. It changes the behavior of the start program. In the middle of the execution, the control is handover to the attached piece of code. After getting executed, it returns to the main execution program. It is unable to identify when the execution got completed. If the piece of code has a program written to capture the user details, then these details may be shared with the hacker remotely without the permission of the user.

2. **Boot Sector Virus**
   These are also known as memory virus. It poisons the boot sector of the system, gets executed each time when the system is booted and before Operating System is loaded. It contaminates other bootable media like floppy disks.

3. **Macro Virus**
   This Virus is programmed using high-level language like Visual Basic (VB). It gets automatically triggered when macros are enabled. Mostly get to see this type of Virus coming through spreadsheets.

4. **Source Code Virus**
   It finds for a source code file and alters it to include virus and spread it.

5. **Encrypted Virus**
   This type of virus makes use of encryption and decryption technique. The Antivirus should not be able to identify that is why it always exists in an encrypted form. It carries the decryption algorithm with itself. Whenever it requires, it gets itself decrypted and spread.

6. **Stealth Virus**
   It is a very complicated virus; changes the code as it is detected. It is difficult to identify and fix. In case it is detected, then this virus tries to fool the user by showing the real code instead of the altered code. – Tunneling Virus: This virus tries to bypass the detection of antivirus scanner by installing itself in the interrupt handler chain. Intercepting programs, remain in the background of an OS and catching such type of virus is difficult.

7. **Multipartite Virus**
   This type of virus is capable of infecting multiple portions of a system, including boot sector, memory, and records. It is unable to detect and fix it.

8. **Armored Virus**
   It is coded with high-level language so that even the antivirus is unable to detect and remove it. It fools the antivirus by giving its fake path instead of the real location where it is available.

- **Trojan**
  Trojans are malicious software programs. It gets installed into the victims Working Hub and keeps sharing the victim's information to the hacker remotely. It also locks the files, serves fraud advertisement, averts traffic, sniff data.

- **Denial of service**
  Denial of service is an attack to make the web server unavailable or crash the entire web server. In this kind of attack, the hacker makes use of bots or zombie machine to flood the web server with lots of requests and make the server come down. The hacker can achieve this in less amount of time.

- **Waterhole attacks**
  In this type of attack, the attacker always tries to know who are the frequent visiting user on website or groups. They mostly target high profile companies this attack as the tendency to poison the members of the targeted victim group. They mainly concentrate on infecting websites with malware and making the target more vulnerable and are challenging to identify.

- **Browser locker**
  The person who his not much into the technological things may easily get trapped into this kind of Attack. This attacker encourages the user to visit their Website or with the attractive web post, make the person forcefully redirect to their Website. Now

the main trap begins from here. The hacker displays a popup message box that takes over the screen and makes it difficult for the visited user to close. The popup always as message like antivirus alert, System Cleanup, and assists the user to visit a malicious Computer support link. The visited victim ends up paying the attacker to kill the virus from their computer.

- **Cross-site scripting**
  A website gets connected to Different servers to optimize their functionalities for better communication. If not worried about confirming their authentication once they switch to another server; this may lead to misuse of the website. Even the hacker may try to inject the Script to take over the control of the site and steal the information of the user.

- **IoT Attacks**
  Everyone is moving towards an era of IoT. Human beings cannot live without the Internet for a minute; also, it as made the life of the Human beings simpler. However, Now, because of new hacking techniques, even it has been infected and been widely used for stealing the Data of the user. A good example is smartwatches, smart TVs, and all smarty gadgets which are built to add happiness in their life now threatening them. Instead of the positive impact, it has created adverse effects on the life of Human beings.

8. ETHICAL HACKING TOOLS

- John the Ripper
- Metasploit
- Nmap
- Wireshark
- OpenVAS
- IronWASP
- Nikto
- SQLMap
- SQLNinja
- Maltego
- AirCrack-ng
- Reaver
- Ettercap
- Canvas
- AirSnort
- Cain and Able
- Kismet
- Net Stumbler
- inSSIDer
- CoWPAttY
- AirJack
- OmniPeek
- Cloud Cracker
- Acunetix WVS — Vulnerability Scanner
- Nmap — Port scanner tool
- oclHashcat — Password cracking tool
- Nessus — Vulnerability Scanner
- Social-Engineer Toolkit
- Netsparker — Web app scanner
- w3af — Web app scanner
- Ghidra — Reverse Engineering Tool
- AndroRAT
- Hack code
- zANTI
- cSploit
- Faceniff
- Shark for Root
- Droidsheep
- DroidBox
- APKInspector
- SSHDroid
- WiFi-Kill
- Kali Linux Hunter
- Fing Network Scanner
- Termux
- ikeyMonitor
- Hoverwatch
- Copy9
- Orbot
- Haven Keep watch
- NetCut
- Arpspoof
- DroidSqli

9. PREVENTIVE MEASURES FOR NEWBIES

1. **Beware of Public WiFi**
   Do not sign in to Public WiFi. Unless and until its a legitimate one. There may be a possibility that hacker may create a Fake WiFi using a reputed name. This method may give a Hacker Entire Details.

2. **Complex Passwords**
   Create a Complex password. This complex Password will prevent from hacking. Even if the hacker tries Brute force attacking may not be able to get the Password.

3. **Change Password often**
   Change the Password every Week. While changing Password, a popup box appears, saying," log out from all devices. "Click, Yes as it Logs out from all the devices when logged in, especially when logged in from friends or colleagues mobile for some work.

4. **Use two-factor authentication**
   Make use of Two Step authentication So that unknown person may not be able to log in as it prevents from stealing the Details.

5. **Read the Privacy policy**
   Read the Privacy policy carefully before registering.

6. **Website Verification**
   Check the Website address before logging. It should have https: [SSL]. Otherwise, avoid logging such website.

7. **Pattern and PIN**
   Make use of a lock pattern or PIN to prevent the third person from spying.

8. **Avoid installation**
   Avoid installing unsafe software and apps it may lead to the stealing of Data.

9. **Use Antivirus**
   Make use of updated antivirus instead of the cracked version. This cracked version may have the virus which may lead to the stealing of Data remotely.

10. **Encrypt Data**
    Encrypt the sensitive documents to prevent it from hacking.

11. **Suspicious link**
    Avoid clicking suspicious links and posts or replying to unknown emails.

12. **Activate Firewall**
    Activate Firewall as it prevents an unauthorized person from accessing.

13. **Remote Access**
    Disable the Remote Access as it prevents an unauthorized person from accessing.

14. **Cleanup Activity**
    Perform the Cleanup activity of PC/Laptop and update outdated drivers and software.

15. **Others**
    Disable auto fill form option Avoid accepting cookies and save password popups.

10. CONCLUSION

The world is moving towards the advancement Of technology. Moreover, there is no control over the Human brain and the Activities which they perform. This paper describes the hacking and the tools used by the hacker to get access to the Data in an unauthorized way. The mentioned preventive measures are used and applied in life may diminish the probabilities of getting hacked.

REFERENCES

[1] B. Sahare, A. Naik, and S. Khandey, "Study Of Ethical Hacking," Int. J. Comput. Sci. Trends Technol., vol. 2, no. 4, pp. 6–10, 2014.

[2] I. G. Hostel and H. Road, "Tcs Employment Application Form," no. 717, 1991.

[3] S. Begum and S. Kumar, "Ijesrt International Journal of Engineering Sciences & Research, Technology a Comprehensive Study on Ethical Hacking," Int. J. Eng. Sci., vol. 5, no. 8, pp. 214–219, 2016.

[4] S. Satapathy and D. Ranjan Patra, "Ethical Hacking," Int. J. Sci. Res. Publ., vol. 5, no. 6, pp. 2250–3153, 2015.

[5] K. B. Chowdappa, S. S. Lakshmi, and P. N.V. S. P. Kumar, "Ethical Hacking Techniques with Penetration Testing,"

[6] K.Bala Chowdappa al, / Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 3, pp. 3389–3393, 2014.

[7] D. Nayyar, "Top 10 operating systems for ethical hackers and penetration testers", Open Source For You, 2019. [Online]. Available: https://opensourceforu.com/2017/02/operatin g-systems-ethical-hackers-penetration-testers/. [Accessed: 20- Jun- 2019].

[8] "What is backtrack? - Quora", Quora.com,2019. [Online]. Available: https://www.quora.com/What-is-backtrack. [Accessed: 20- Jun- 2019].

[9] K. Hess, "BackTrack Linux: The Ultimate Hacker's Arsenal » ADMIN Magazine," ADMIN Magazine, 2019. [Online]. Available: http://www.admin-magazine.com/Articles/BackTrack-Linux-The-Ultimate-Hacker-s-Arsenal. [Accessed: 21- Jun- 2019].

[10] "BackTrack five tutorial Part I: Information gathering and VA tools," ComputerWeekly.com, 2019. [Online]. Available: https://www.computerweekly.com/tip/BackT rack-5-tutorial-Part-I-Information-gathering-and-VA-tools. [Accessed: 21- Jun- 2019].

[11] H. Chaudhary, "Top Best Operating Systems (OS) for Hackers - Ultimate Tech," Ultimate

[12] I1.wp.com, 2019. [Online]. Available: https://i1.wp.com/www.ultimatetech.org/wp-content/uploads/2017/10/Top-Best-Operating-Systems-OS-for-Hackers.jpg?resize=696%2C392&ssl=1. [Accessed: 21- Jun- 2019].

[13] "10 Common Hacking Techniques", YouTube, 2019. [Online]. Available: https://www.youtube.com/watch?v=V3CTfJ2 ZP7M. [Accessed: 21- Jun- 2019].

[14] A. Shekhar, "Top 10 Common Hacking Techniques You Should Know About,", Fossbytes, 2019. [Online]. Available: https://fossbytes.com/hacking-techniques/. [Accessed: 22- Jun- 2019].
[15] "The most common types of hacking on the Internet," NordVPN, 2019. [Online]. Available: https://nordvpn.com/blog/hacking/. [Accessed: 22- Jun- 2019].
[16] A. Die, "8 Most Common Website Hacking Techniques You Should Know", Cobweb Security - WebDefender website security, 2019. [Online]. Available: https://cobweb-security.com/security_lessons/8-common-website-hacking-techniques-know/. [Accessed: 22- Jun- 2019]. "Types of Viruses - GeeksforGeeks," GeeksforGeeks, 2019. [Online]. Available: https://www.geeksforgeeks.org/types-of-virus/. [Accessed: 24- Jun- 2019].
[17] WikiHow, "4 Ways to Prevent Hacking - wikiHow." [Online]. Available: https://www.wikihow.com/Prevent-Hacking. [Accessed: 26-Jun-2019].
[18] "6 Expert Tips to Avoid Getting Hacked | Inc.com." [Online]. Available: https://www.inc.com/jon-levy/6-expert-tips-to-avoid-getting-hacked.html. [Accessed: 26-Jun-2019].
[19] J. Rampton, "12 Tips to Protect Your Company Website From Hackers," Entrepreneur.com, 2015. [Online]. Available: https://www.entrepreneur.com/article/241620[Accessed: 26-Jun-2019].
[20] R. Burn-Callander, "Seven ways to avoid being hacked," Telegraph.co.uk, 2019. [Online]. Available: https://www.telegraph.co.uk/finance/yourbusiness/11393773/Seven-ways-to-avoid-being-hacked.html. [Accessed: 27- Jun- 2019].
[21] G. Beall, "How to prevent your company from getting hacked in 2018", The Next Web,
[22] 2019. [Online]. Available: https://thenextweb.com/contributors/2017/10/25/prevent-company-getting-hacked-2018/. [Accessed: 27- Jun- 2019].
[23] "21 Hacking apps for the Android phone: List of best apps 2019", Opentech Info, 2019. [Online]. Available: https://www.opentechinfo.com/hacking-apps/. [Accessed: 27- Jun- 2019].
[24] "What is SQL Injection (SQLi) and How to Prevent It," Acunetix, 2019. [Online]. Available: https://www.acunetix.com/websitesecurity/sql-injection/. [Accessed: 23- Jun- 2019].
[25] "5 Best Hacking Tools For Windows 10 - (2018 Edition)", TechWorm, 2019. [Online]. Available: https://www.techworm.net/2018/07/5-best-hacking-tools-windows-10.html. [Accessed: 27- Jun- 2019].
[26] "Best 40 Hacking Apps for Android Phones No Root 2019", Jihosoft.com, 2019. [Online]. Available: https://www.jihosoft.com/android-tips/android-hacking-apps.html. [Accessed: 27- Jun- 2019].
[27] "Ethical Hacking Tools," www.tutorialspoint.com, 2019. [Online]. Available: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tools.htm. [Accessed: 27-Jun-2019].
[28] G. List and S. 2019, "Selected 38 Best Android Hacking Apps And Tools Of 2019", TechLog360, 2019. [Online].Available: https://techlog360.com/best-android-hacking-apps/. [Accessed: 27- Jun-2019].
[29] H. NEWS and B. Windows, "Best Hacking Tools for Windows - Hack Ware News," Hack Ware News, 2019. [Online]. Available: https://hackwarenews.com/best-hacking-tools-for-windows/. [Accessed: 27- Jun-2019].
[30] "SecurityTrails | Top 15 Ethical Hacking Tools Used by Infosec Professionals", Securitytrails.com, 2019. [Online]. Available: https://securitytrails.com/blog/top-15-ethical-hacking-tools-used-by-infosec-professionals. [Accessed: 27- Jun- 2019].
[31] "SecurityTrails | Top 15 Ethical Hacking Tools Used by Infosec Professionals", Securitytrails.com, 2019. [Online]. Available: https://securitytrails.com/blog/top-15-ethical-hacking-tools-used-by-infosec-professionals. [Accessed: 27- Jun- 2019].
[32] A. Verma, "13 Best Hacking Tools Of 2019 For Windows, Linux, macOS", Fossbytes,
[33] 2019. [Online]. Available: https://fossbytes.com/best-hacking-tools-of-
[34] 2016-windows-linux-mac-osx/. [Accessed: 27- Jun- 2019].