National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040; Impact Factor: RJIF 5.22
Received: 26-05-2020; Accepted: 11-06-2020; Published: 27-06-2020
www.nationaljournals.com
Volume 5; Issue 2; 2020; Page No. 33-37

All about Hacking and it's Upcoming Trends

Nidhi
Assistant Professor, Department of Computer Science, Dasmesh Girls College Chak Alla Baksh, Mukerian, Punjab, India

Abstract
Internet has opened a new world. It is a manifestation of never-ending innovation and creativity. It is a source of information, a social platform, and a business network but Information security has become one of the most important concepts in our information and technology driven world. Cyber criminals have evolved several techniques to threat privacy and integrity of bank accounts, businesses, and organizations database. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer. White hat hacking is an exciting concept where the premise is that if you want to catch a criminal you must be able to think like one to stay one step ahead. This paper describes what is ethical hacking, what are the types of Hackers, hacking history, techniques used in hacking.

Keywords: vulnerabilities, cracker, ethical hackers, cyber-attack, code breakers, phreaker, script kiddies, hacktivist

1. Introduction

What is hacking?

Hacking often refers to the unauthorized intrusion into a network or computer; normally carried out by one or more "hackers." However, a hacker can be anyone. They can be an individual like you or me. They can work solo or employed by an organization that has the motive to disrupt something or cause havoc—unnecessarily. Often, they look to alter security systems to achieve their goal, which differs from the actual purpose of the system. Many organizations hire hackers as a part of their staff. These hackers use their skills to find flaws, vulnerable areas, and weak spots in the organization's security system. This is done to find and fix the weaknesses and prevent malicious hackers from breaking in the security system.

- The first hacker was appeared in 1960's at the Massachusetts Institute of Technology (MIT) • during the 1970's, a different kind of hacker appeared: phone phreaker or phone hacker.
- Hackers are most often programmers. They gather advanced knowledge of operating systems and programming languages and discover loopholes within systems and the reasons for such loopholes.
- The terms hacker and cracker are often used interchangeable although there is an important difference. A cracker is defined as someone who breaks into a system and has malicious intent. Crackers are the subset of the hacking community that attempt to circumvent security controls so they can gain unauthorized access to information and confidential material. Once they are able to sidestep security controls and exploit a flaw in the system, they can do any number of harmful things. What separates a cracker from a hacker is that crackers are those with destructive or evil intent while hackers and more specifically, white hat hackers have something very different in mind.

2. Hacking Timeline

Table 1

▪ **1834** — **French Telegraph System** — a pair of thieves hack the French Telegraph System and steal financial market information, effectively conducting the world's first cyber-attack.
▪ **1870** — **Switchboard Hack** — a teenager hired as a switchboard operator is able to disconnect and redirect calls and use the line for personal usage.
▪ **1878** — **Early Telephone Calls** — Two years after Alexander Graham Bell invents the telephone, the Bell Telephone Company kicks a group of teenage boys off the telephone system in New York for repeatedly and intentionally misdirecting and disconnecting customer calls.
▪ **1903** — **Wireless Telegraphy** — During John Ambrose Fleming's first public demonstration of Marconi's "secure" wireless telegraphy technology, Nevil Maskelyne disrupts it by sending insulting Morse code messages discrediting the invention.
▪ **1939 — military Code breaking** — Alan Turing and Gordon Welchman develop BOMBE, an electro-mechanical machine, while working as code breakers at Bletchley Park. It helps to break the German Enigma codes.
▪ **1940 —** First Ethical Hacker, Rene Carmille, a member of the Resistance in Nazi-occupied France and a punch-card computer expert who owns the machines that the Vichy government of France uses to process information, finds out that the Nazis are using punch-card machines to process and track down Jews, volunteers to let them use his, and then hacks them to thwart their plan.
▪ **1955 — Phone Hacker** — David Condon whistles his "Davy Crockett Cat" and "Canary Bird Call Flute" into his phone, testing a theory on how phone systems work. The system recognizes the secret code, assumes he is an employee, and connects him to a long-distance operator. She connects him to any phone number he requests for free.
▪ **1962 — Allan Scherr —** MIT sets up the first computer passwords, for student privacy and time limits. Student Allan Scherr makes a punch card to trick the computer into printing off all passwords and uses them to log in as other people after his time runs out. He also

shares passwords with his friends, leading to the first computer "troll." They hack into their teacher's account and leave messages making fun of him.
▪ **1983— Kids'** Games Movie "War Games" introduces public to hacking.
▪ **1986**— Congress passes Computer Fraud and Abuse Act; crime to break into computer systems.
▪ **1988**— The Morris Worm Robert T. Morris, Jr., launches self-replicating worm on ARPAnet.
▪ **1995**— The Mitnick Takedown: Arrested again; charged with stealing 20,000 credit card numbers.
▪ **1999** — E-commerce Company attacked; blackmail threats followed by 8 million credit card numbers stolen.
▪ **2013**—In early October of 2013 by security blogger Brian Krebs, Adobe originally reported that hackers had stolen nearly 3 million encrypted customer credit card records, plus login data for an undetermined number of user accounts.
▪ **2017**—The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

3. Types of Hackers and What They Do

Table 2

Types of Hackers		
Black Hat' Hackers: The Ba d Guys	Definition: They are often called as *Crackers*. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious actions.	Aim: The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
White Hat' Hackers: The Good Guys	White-hat hackers are often referred to as ethical hackers. This individual specializes in ethical hacking tools, techniques, and methodologies to secure an organization's information systems. Unlike black-hat hackers, ethical hackers exploit security networks and look for backdoors when they are legally permitted to do so. White-hat hackers always disclose every vulnerability they find in the company's security system so that it can be fixed before they are being exploited by malicious actors.	Aim: A desire to help businesses, along with a passion for finding holes in security networks.
Gray Hat Hackers: The In-the-Middle Guys	Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not	Aim: Grey Hat hackers have all the skills of a Black and a White Hat hacker. The difference is, they don't care about stealing from people, nor do they particularly want to help people. Instead, they like to play with systems and enjoy the challenge of finding gaps, breaking protections and generally just find hacking fun.
Script Kiddies: The In-It-for-Fun Guys	Script Kiddies: They are the most dangerous people in terms of hackers. A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers. They attempt to attack computer systems and networks and deface websites.	Aim: Their main purpose is to impress their friends and society. Generally, Script Kiddies are juveniles who are unskilled about hacking.
Green Hat Hackers: The Beginners	Green hat hackers are newbies and they are working to improve their skills every day so they can become better. The green hat has something to prove and often gets chided by the hacking community if they ask basic questions. Yet, their desire to learn keeps them asking. They may idolize well-known black hats and are desperate to elevate themselves to the real world of hacking. Even though they lack skills, they can still cause problems.	Aim: Green Hat hackers are all about the learning. They are new to the world of scripting, coding and hacking in general, so you probably won't find one attacking. Instead, they hang around online message boards asking questions of more developed hackers, honing their skills
Red Hats Hackers: The caped crusaders of the cyber world.	They are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate. They become ruthless while dealing with malware actions of the black hat hackers. Red hat hacker will keep on attacking the hacker aggressively that the hacker may know it as well have to replace the whole system.	The objective of a red hat hacker is to find black hat hackers, intercept and destroy their schemes.

Blue Hat Hacker	Blue Hat hackers often take existing code for malware and viruses they find online, then modify it to meet their needs. They will use this code to target the business or individual they feel has wronged them and inflict their revenge. Generally, only a problem if you've made someone very, very angry. This could be a customer, supplier or employee – anyone who might be so angry that they want to 'make you pay	Blue Hat hackers payback to those who have challenged them or angry them. Like the Script Kiddies, Blue hat hackers also have no desire to learn.
Hacktivist: The Political Guys	These are also called the online versions of the activists. Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends. A hacktivist can be considered a sub-group of black hats. They use technology to exact attacks for political reasons	Aim: To gain unauthorized access to government's computer files and networks for further social or political ends.

4. Techniques used by hackers

There are many techniques that hackers use to gain unauthorized access to information.

4.1 Scanning/probing: A scan or probe is considered to be a security compromise where a hacker may attempt to systematically find those communication ports along the network that are open and able to return information. Once the hacker knows what ports are open and what information can return, they have an insight into where the network may be exposed for a future attack.

4.2 Session Hijacking. When users attempt to establish one-time remote connections to other computers on a network, hackers look to steal these sessions so they can have the same privileges as the authorized user.

4.3 Key loggers: key-loggers are most often used for stealing passwords and other confidential information. Key-logging is the process of recording the keys struck on keyboard, typically covertly, so that person using the keyboard is unaware that his actions are being monitored. Data cab be retrieved by the person operating the logging program.

4.4 Bait and switch: Bait and Switch hacking is a technique on the rise due to explosion of Internet based Content marketing. A bait and Switch attack occurs when victims are told they are downloading and running a piece of safe and legitimate content, which is the switched (usually by way of a redirect) to something malicious. It 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.

4.5 Cookie theft: What are computer cookies? A cookie is a tiny file that websites store on your computer. They are normally perfectly harmless – and quite useful too. In fact, many of the websites you use every day rely on cookies to work properly. Cookies were designed to be a reliable mechanism for websites to remember information or to record the users browsing history. These tiny text files can be used for storing login information, credit card information and help advertisers show ads they think will be relevant to your preferences.

Cookies do not directly display passwords; instead, they contain a hash that stores your password. When a password has been hashed, it has been scrambled so only the website it came from can read it. The website uses a unique encryption algorithm to encode and decode the hash. Stealing your cookies may be just as good. By installing your cookies with hashed passwords into their web browser, the criminal can immediately access your account, no login required.

4.6 Click-Jacking: Click-jacking (classified as a User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages.

Consider the following example

A web user accesses a decoy website (perhaps this is a link provided by an email) and clicks on a button to win a prize. Unknowingly, they have been deceived by an attacker into pressing an alternative hidden button and these results in the payment of an account on another site. This is an example of a click jacking attack.

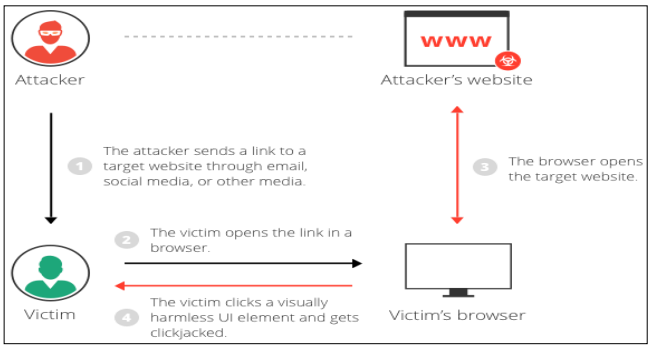

Fig 1

4.7 Phishing: The scam, which involves criminals sending messages that masquerade as legitimate organizations, targets hundreds of millions of organizations every day. The messages direct recipients to a bogus website that captures their personal information or contain a malicious attachment. 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

4.8 Brute Force Attack: A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered. The longer the password, the more combinations that will need to be tested. A brute force attack can be time consuming; however, if the password is weak it could merely take seconds with hardly any effort. Weak passwords are like shooting fish in a barrel for attackers, which is why all organizations should enforce a strong password policy across all users and systems.

4.9 SQL injection: SQL injection usually occurs when you ask a user for input, like their username/user ID, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database. SQL injection is a code injection technique that might destroy your database. SQL injection is the placement of malicious code in SQL statements, via web page input. An attacker can include their own SQL commands which the database will execute

4.10 Trojan: A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems.

4.11 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 smart watches, 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.

5. New Hacking Trends

- **Cloud Vulnerability**

  Loss of data: there is always the risk that sensitive data is in somebody else's hands. If the security of a cloud service is breached, hackers could potentially gain access to intellectual property or other personal files. **Malware infections:** Due to the high volume of data stored on the cloud, which requires an internet connection to store this data, anybody using cloud services is potentially at risk of cyber-attacks. An increasingly common threat is Distributed Denial of Service (DDoS) attacks, whereby hackers send unprecedented volumes of traffic to a web-based application, thereby crashing the servers. **Crypto jacking:** is a new form of cyber-attack, Crypto jacking can be very tricky to spot and deal with. The major issue here is the fact that when hackers use computing resources from your cloud system means your operation will be slowed down, but (crucially) it will continue to work. This means that it can seem as if nothing malicious is happening and that perhaps the computers are just struggling with their processing power.
- **Denial of service:** One of the most damaging threats to cloud computing is a denial of service (DoS) attack. These can shut down your cloud services and make them unavailable both to your users and to customers, but to your staff and business as a whole. Cybercriminals can flood your system with a very large amount of web traffic that your servers are not able to cope with. This means that the servers will not buffer, and nothing can be accessed. If the whole of your system runs on the cloud, this can then make it impossible for you to manage your business.

- **AI-Enhanced Cyberthreats**

1. AI cyberattacks are becoming a rising security threat both for everyday people and large government agencies. It is now becoming easier for hackers to develop machine algorithm hacking methods or use botnets to their full capabilities as those methods spread across the web.

   Overall, machine learning algorithms are becoming more complex and accurate. Every time a bot system makes a spam attack, it becomes better when it tries again.
2. Cyber security agencies and website developers will need to respond with far more innovative solutions to effectively protect their users' data.

- **AI Fuzzing:** AI fuzzing integrates AI with traditional fuzzing techniques to create a tool that detects system vulnerabilities. This can be a boon or a bane. Though AI fuzzing can help enterprises detect and fix the exploitable vulnerabilities in their system, it can also be used by cybercriminals to start, automate, and accelerate zero-day attacks.
- **Machine Learning Poisoning:** If a hacker targets a machine learning model and injects instructions into it, the system becomes vulnerable to attacks. Machine learning models typically use data that is crowd-sourced or taken from social media. They also exploit user-generated information such as satisfaction ratings, purchasing histories, or web traffic. Cybercriminals engaging in MI poisoning could potentially use malicious samples or introduce backdoors or Trojans to poison training sets and compromise the system.

- **5G implementation**

With the bandwidth that 5G technology enables, data volumes and the number of connected devices and sensors is set to explode. Electronic health applications will collect data about a user's wellbeing, new car technology will monitor a user's movements, and smart applications will collect information about how users live and work. With so many personal data being collected from us, 5G technology will mean high levels of security against breaches and data theft will be required.

- **Mobile apps**

Mobile phones will be a big target in 2020, with a multitude of apps now being 'must-installs' for a large percentage of the population. These apps are often downloaded with no concern for security at all. One such app is the Chinese-developed TikTok – an app that allows the user to create short videos and is immensely popular with young people. TikTok has been found to have many vulnerabilities, some of which have been closed. Regardless, TikTok is, in the United States of America, being considered as a threat to national security, particularly so with the likelihood of the Chinese government's access to the application's data and user profiles.

Preventive Measures

- Beware of Public WiFi
- Use two-factor authentication
- Avoid installation
- Encrypt Data
- Avoid clicking suspicious links
- Activate Firewall
- Disable the Remote Access
- Make use of updated antivirus
- Use Complex Passwords
- Clean Cookies Periodically
- Go to the official website of the online retailer directly.

- Use VPN (virtual private network)
- Examine the privacy policies and security features before using any app.

Conclusion

In the era of internet and advancement in every field, everyone is using internet for their day-to-day work. Internet, as a whole can be seen as technology that has greatly enhanced our lives. Nowadays, online banking is practically the norm. While the introduction of the Internet led to many benefits, unfortunately, it also came with its own set of problems. Most significantly, these problems can negatively affect your security and privacy. This paper describes about hacking and the tools used by the hacker to get access to the Data. Preventive measures that can be used in day-to-day life to keep our data safe from hackers.

References

1. https://www.geeksforgeeks.org/5-common-hacking-techniques-used-by-hackers/
2. https://antivirus.comodo.com/blog/comodo-news/hacking-definition-and-its-types/
3. https://www.guru99.com/what-is-hacking-an-introduction.html
4. https://www.malwarebytes.com/hacker/
5. https://www.tutorialspoint.com/internet_technologies/internet_security_overview.htm
6. https://madhavuniversity.edu.in/ethical-hacking.html
7. https://www.digitalvidya.com/blog/types-of-hacking/
8. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
9. https://www.eccouncil.org/ethical-hacking/
10. https://www.sciencedirect.com/topics/computer-science/white-hat-hacker
11. https://digitalcommons.pace.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1012&context=honorscollege_theses
12. https://www.techfunnel.com/information-technology/different-types-of-hackers/
13. https://www.pentasecurity.com/blog/6-types-hackers-online/#:~:text=Unlike%20a%20script%20kiddie%2C%20the,inner%20workings%20of%20the%20web
14. https://alpinesecurity.com/blog/hacker-hat-colors-an-inside-look-at-the-hacking-ecosystem/
15. https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/
16. https://www.bridewellconsulting.com/different-types-of-hackers-and-what-they-mean-for-your-business
17. https://www.geeksforgeeks.org/types-of-hackers/
18. https://www.guru99.com/what-is-hacking-an-introduction.html#:~:text=Types%20of%20Hackers,with%20knowledge%20of%20computer%20security.&text=Grey%20hat%3A%20A%20hacker%20who,ethical%20and%20black%20hat%20hackers.
19. https://www.slideshare.net/punitpandey9/hacking-and-types-of-hacker-80376500
20. https://www.herjavecgroup.com/history-of-cybercrime/
21. https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/
22. https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/Clickjacking.png
23. https://en.wikipedia.org/wiki/Clickjacking#:~:text=Clickjacking%20(classified%20as%20a%20User,control%20of%20their%20computer%20while
24. https://www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,credit%20card%20details%2C%20and%20passwords.
25. https://en.wikipedia.org/wiki/Brute-force_attack
26. https://www.w3schools.com/sql/sql_injection.asp
27. https://www.thesslstore.com/blog/cloud-security-5-serious-emerging-cloud-computing-threats-to-avoid/
28. https://www.infoq.com/articles/ai-cyber-attacks/
29. https://vittana.org/12-pros-and-cons-of-internet