International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 4, Issue 1, pp 5-8, January-2020

Hacking on Crime with Workable Solution: A Survey

[1]Payal Wade, [2]Radhika Joshi, [3]Prof. S. K. Totade

[1,2]P.G. Student, Final Year MCA, Department of MCA, Vidya Bharati Mahavidyalaya, Amravati (M.S), India
[3]Professor, Final Year MCA, Department of MCA, Vidya Bharati Mahavidyalaya, Amravati (M.S), India

***Abstract* - The study conducted to investigate the hacking crime & Workable solution. Hacking identifies vulnerabilities in computer systems or networks in order to exploit these vulnerabilities for access. Example of hacking: use of the password hacking algorithm to access a system. Computers have become a prerequisite for the success of a business. It is not enough to have an isolated computer system. They must be networked to facilitate communication with external companies. They must be networked to facilitate communication with external companies. Hacking means using computers to commit fraudulent acts such as fraud breach of privacy, theft of business / personal information, etc. Cybercrime costs many organizations millions of dollars each year. Businesses must protect themselves from such attacks.**

Keywords: Hacking, Phishing, Computer crime, Computer Security, cyber fraud, Prevention of cyber-crime.

I. Introduction

In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer network. Hackers can be motivated for a variety of reasons, including: B. Profiting, protesting, challenging, rejoicing, or assessing these weaknesses to eliminate them. The subculture that has grown up around pirates is often called underground computing and is now a well-known community. Although there are other uses of the global hacker in computer security, for example For example, referring to a person with an advanced understanding of computers and computer networks, they are rarely used in the general context. They are subject to the hackers' long-standing controversy over the true meaning. In this controversy, the term hacker is taken up by computer programmers who argue that an intrusion, whether by computer criminals (black hats) or computer security experts (white hats), is more correctly labeled as a hacker. Some hackers with white hats who claim to deserve the little hacker and these only black hats should be called "crackers". Hacking identifies vulnerabilities in computer systems or networks in order to exploit these vulnerabilities for access. Example of hacking: - Use algorithms to crack passwords to access a system. Computers have become mandatory to run a successful business. It is not enough to have isolated computer systems. They must be networked to facilitate communication with external companies. This exposes them to the outside world and to piracy. Hacking means the use of computers to commit fraudulent acts such as fraud, breach of privacy, theft of business / personal information, etc. Cybercrimes cost many organizations millions of dollars each year. Businesses must protect themselves from such attacks.

On the one hand, hacking describes the activities of individuals, organizations and nations in order to gain unauthorized access to computer and technological systems. These activities may include modifying or changing software and system hardware to perform activities that are neither intended by the creator nor the original intentions of the creator.

On the other hand, and in a more positive connotation, it refers to the usual activities of someone who has exceptional skills and likes to research and analyze the most intimate subtleties of computer programming.

If we look at both sides of the definition, we can see that the general term is not definitively condemned with a negative connotation. In fact, a distinction has been made in the IT world based on the nature of the hacker's objectives. As such, hackers have been mischievously defined as crackers.

II. Literature Review

In password security: An empirical investigation into ecommerce passwords and their crack times. Author proposed that strong passwords are essential to the security of any e-commerce site as well as to individual users. Without them, hackers can break in a network and stop cavallies working that assist end user and keep companies operating. For most e-commerce sites, end users have the incumbency of creating their own passwords and often do so without conveyance from the web site or system chairperson. One fact is well known about password procreation –consumers do not create long or labyrinthine passwords because they cannot remember them.

III. Why Do People Hack Computers?

When someone hacks a computer or network system, it’s typically for one of three main reasons:

Figure 1: Hacking Computer

Hacking for fun: Some hackers try to work on computers, servers or network systems just to satisfy themselves. Others may think they have to prove something to their colleagues or friends and have to hack something just to meet the challenge.

Hacking to steal: Another reason to hack into a system is to steal information or money. A large part of hacking attempts fall into this category. Banks and large businesses are common targets for hacking jobs, but sometimes small businesses or a person's computer are also affected.

Hacking to disrupt: There are also hackers, including groups of hackers; the goal of a business is to disrupt business, create chaos, and just be a nuisance. These groups often try to report with their hacking, point out security gaps, or generally show rejection for the company itself.

IV. How to Prevent Hacking?

4.1 Use a full-service internet security suite

For example, Norton Security provides real-time protection against existing and new malware, including ransoms and viruses, and protects your personal and financial information when you log in.

4.2 Use strong Passwords

Do not repeat your passwords on different websites, but change them regularly. Make them complex. This means that you are using a combination of at least 10 letters, numbers and symbols. You can use a password management application to lock your passwords.

4.3 Keep your software updated

This is particularly important with your operating systems and Internet security software. Cybercriminals often use known exploits or bugs in your system.

4.4 Manage your social media settings

Protect your personal and private data. Social engineering cybercriminals can often access your personal data with only a few data points. So the less you share in public, the better. For example, if you publish your pet's name or reveal your mother's maiden name, you can reveal the answers to two common safety questions.

4.5 Strengthen your home network

It is a good idea to start with a secure encryption password as well as a virtual private network. A VPN encrypts all traffic that leaves your devices until it reaches its destination. If cybercriminals manage to hack your line of communication, they will only intercept encrypted data. It is a good idea to use a VPN when using a public Wi-Fi network, whether in a library, cafe, hotel or airport.

4.6 Keep up to date on major security breaches

If you're dealing with a merchant or have an account on a compromised website, find out what information hackers accessed and change your password immediately.

4.7 Take measures to help protect yourself against identity theft

Identity theft occurs when someone falsely accesses your personal information fraudulently or descriptively, usually for economic reasons. How? You Might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That’s why it’s important to guard your personal data. A VPN - short for a virtual private network - can also help protect the data you send and receive online, especially if you access the Internet via public WiFi.

4.8 Know that identity theft can happen anywhere

It is wise to know how to protect your identity while traveling. There are many things you can do to prevent criminals from disclosing your personal information.

4.9 Keep an eye on the kids

Just like you want to talk to your kids online, you want to protect them from identity theft. Identity thieves often target children because their social security number and credit rating are often hot. You can protect yourself against identity theft by carefully sharing your child's personal information. It is also wise to know what to look for when your child's identity is compromised.

4.10 Know what to do if you become a victim

If you think you may be a victim of cybercrime, you should tell the local police and, in some cases, the FBI and the Federal Trade Commission. This is important, even if the crime seems minor. Your report can help the authorities investigate or prevent criminals from exploiting others. If you think cybercriminals have stolen your identity. Here are some steps to consider.

V. Future Scope

One can develop such software or technologies that provide more security to prevent piracy, and people can use the Internet safely. We need to teach students about piracy so that they can embrace piracy in a positive way.

VI. Phases of Hacking

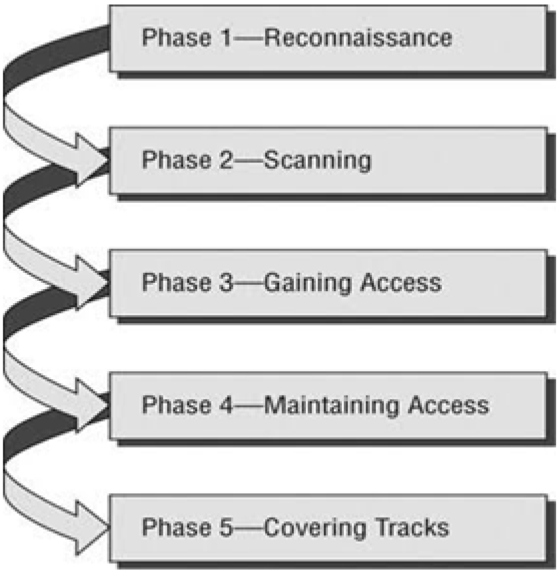

Figure 2: Phases of Hacking

6.1 Reconnaissance

This is the first step of Hacking. It is also called as Footprinting and information gathering phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,

- Network
- Host
- People involved

There are two types of Footprinting:

- **Active:** Directly interacting with the target to gather information about the target. E.g. Using Nmap tool to scan the target
- **Passive:** Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

6.2 Scanning

Three types of scanning are involved:

- **Port scanning:** This phase involves scanning the target for the information like open ports, live systems, and various services running on the host.
- **Vulnerability Scanning:** Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools.

6.3 Gaining Access

In this phase, an attacker uses various tools or methods to break into the system / network. After accessing a system, he must extend his administrator rights in order to install the application he needs, modify data or hide data.

6.4 Maintaining Access

Hackers can simply hack the system to show that it is vulnerable, or it can be so malicious that it wants to maintain or maintain the connection in the background without the knowledge of the user. This can be done with Trojans, root kits, or other malicious files.

6.5 Clearing Track

No thief wants to be caught. A smart hacker always removes all the evidence so that no one later finds traces that lead him.

VII. Conclusion

In summary, hacking classified information through cybercrime is becoming increasingly important for national and personal security in order to stay up to date with new hacking technologies. Piracy is becoming a growing problem as the exchange and dissemination of information via the Internet and digital technologies increase. The exchange and sharing of data poses new challenges to social control in society, as these crimes cannot be easily exposed and are therefore difficult to punish. Ultimately, educating individuals in society about the dangers and the different types of hacking and cybercrime creates wide public oversight of small and large-scale crimes, which increases the chances of law enforcement and prevention.

REFERENCES

[1] Kharat, Shital Prakash. "Cyber Crime–A Threat to Persons, Property, *Government and Societies*." (2017).

[2] Cazier, Joseph A., and B. Dawn Medlin. "Password security: An empirical investigation into e-commerce passwords and their crack times." *Information Systems Security* 15.6 (2006): 45-55.

[3] Zakaras, Matthew R. "International computer crimes." *Revue international de droit pénal* 72.3 (2001): 813-829.

[4] Ye, Peisong, and Guangxue Yue. "Security Research on WEP of WLAN." *Proceedings of the Second International Symposium on Networking and Network Security (ISNNS'10) Jinggangshan*, PR China. 2010.

[5] Icove, David, Karl Seger, and William VonStorch. Computer crime: a crimefighter's handbook. *California: O'Reilly & Associates*, 1995.

[6] Casey, Eoghan. Digital evidence and computer crime: Forensic science, computers, and the internet. *Academic press*, 2011.

[7] Carter, David L. "Computer crime categories: how techno-criminals operate." *FBI law enforcement bulletin* 64.7 (1995): 21.

[8] Garber, Lee. "Denial-of-service attacks rip the Internet." *IEEE Computer* 33.4 (2000): 12-17.

[9] Warren, Matthew, and William Hutchinson. "Cyber attacks against supply chain management systems: a short note." *International Journal of Physical Distribution & Logistics Management* 30.7/8 (2000): 710-716.

[10] Barber, Richard. "Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated." *Computer Fraud & Security* 2001.3 (2001): 9-12.

[11] Vladimirov, Andrew, Konstantin V. Gravrilenko, and Andrei A. Mikhailovskiy. Wi-Foo: the secrets of wireless hacking. *Pearson Education*, 2004.

Citation of this Article:

Payal Wade, Radhika Joshi, Prof. S. K. Totade, “Hacking on Crime with Workable Solution: A Survey” Published in *International Research Journal of Innovations in Engineering and Technology (IRJIET)*, Volume 4, Issue 1, pp 5-8, January 2020.

****