




Hacking a Loophole in Computer Security

– Sohail Hussain

Master of Computer Applications (MCA),RV College of Engineering, Bangalore, karnataka

 <https://orcid.org/0000-0002-2569-6927>  sohailhussain5@gmail.com

Article History

Paper Nomenclature:

Experiential Research Papers (ERP)

Paper Code: CYBNMV1N6NOV2019ERP1

Submission Online: 03-Nov-2019

Manuscript Acknowledged: 09-Nov-2019

Originality Check: 10-Nov-2019

Originality Test Ratio: 0%

Peer Reviewers Comment: 14-Nov-2019

Blind Reviewers Remarks: 15-Nov-2019

Author Revert: 21-Nov-2019

Camera-Ready-Copy: 22-Nov-2019

Editorial Board Citation: 27-Nov-2019

Published Online First: 22-Jan-2020

Hacking can be used by any intruder to exploit a system and for unauthorised access on a system. To prevent it is to know about it and learn it. One needs to understand the intruder's tactics and attacks. One cannot protect the system from threats unless they are aware of the same. The objective of this paper is to find various attacks; a hacker can use to exploit a system. As it is necessary to know the attacks to prevent it and further for developing anti-hack software. The more you know about the attacks of the intruders the more you prevent and your system will be secured.

Keywords : Hacking | System Security | Techniques

Introduction:

Hacking is a process to gain unauthorised access on a secured system. It can be done by various malicious attacks. It is the act of exploiting the weakness that exists in a system or a network.

Use hacking for identifying weakness and threats in computer security. Due to the increasing number of attempts to maliciously break into computer systems the businesses, organizations and government agencies aimed at protecting their computer and information systems from hackers.

A hacker is a person who tries to understand how the computer system or the software program works, so that he can find loopholes and control the computer by exploiting vulnerabilities in it.

In this paper I gathered information about what Ethical hacking and How

an intruder use it and what attacks an Ethical hacker use to hack any target.

Understanding the Need to Hack Your Own Systems [1]

A. Try to understand intruders Techniques

You cannot properly protect your system from threats you do not understand. The goal is to identify and prevent destruction so that intruders do not harm the system. To track a hacker, you must think like a hacker.

B. Hackers Types

1. *White Hat Hacker:* A white hat hacker is someone who uses his skills only for defensive purposes such as penetration testing. They work for the security of their information systems in offices. They have a great knowledge of the company and its network.
2. *Black Hat Hacker:* A black hat hacker is someone who always

uses his skills for offensive purposes. They work to steal money or personal information by unauthorised access. They are very good to do penetration testing.

3. *Grey Hat Hacker:* A grey hat hacker is someone who is both white hat and black hat hacker. They use their knowledge and skills both for defensive and offensive purposes.

C. Types of Hacking

1. *Local Hacking:* This type of hack is done by running others system and attaching pen drive to hack it by using Trojans and virus file in the pen drive.
2. *Social Engineering:* This Technique uses person's presence of mind to get confidential data. For security never tell your passwords and confidential information on phone



attacker may pretend to be known person.

3. *Remote Hacking:* It is done from anywhere from any system remotely and using vulnerabilities in the target system.

Techniques

The techniques used to remotely access any system by unauthorised access are described as below.

A. Vulnerability Assessment

Vulnerability is the loophole or backdoors in the system. Vulnerability assessment is done to find all possible vulnerabilities which can be used for unauthorized access on the system.

It is the first step from where the hacking process start in which all information is collected.

Hackers can test many of the vulnerabilities identified during the vulnerability assessment to calculate the associated threats and risks.[2]

B. Passive scanning

It finds information of the target without having contact with the tester and the target. It does not work when traffic and data flow is running and sending. It does not alert security mechanism and users. It is mainly

1. *Attacking the company's website for getting* detailed workflow and information and confidential data
2. *Attacking the social networking site* is done when the user is offline to steal account information

C. Active scanning

This technique completes its work with prior information to the target. This uses the data and traffic sent and scans it.

It target's public with scanning tools, which might include:

1. *Social engineering:* This technique uses person mentality to get private information. It is achieved by pretending to be a known person and asking personal information from the target.
2. *Traffic Sniffing:* It captures every packet that flows in the network. It can identify the Internet Protocol.

D. Operating System Fingerprinting [2]

It is used to identify victim Operating System like windows, Linux, UNIX. It also identifies the OS type. This helps us in pre-attack preparation and for good attacks. In this packets send to target and wait for response as different OS respond to packets in different ways it identifies the OS type.

It can be also identify the OS by sniffing technique by analysing the network packets and traffic.

- E. *Conducting an Insider Attack:* In this technique we have to work inside the target company as an employee in the open in the presence of other employees. The security within the organisation is weak and vulnerabilities and loopholes can be found.

Methodology

Hacking tools used to crack, prevent, detect and find the weakness in the system.

This processes is used to hack a system-[3]

1. Deciding Testing methods
2. Gathering confidential data
3. Map the network
4. Scan the System
5. Find the open ports
6. Detecting Vulnerabilities
7. Penetrate the System

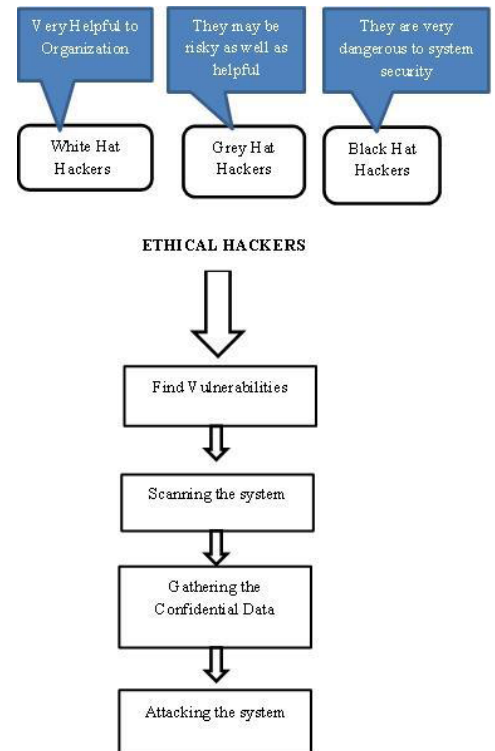


Fig1. Hackers types and steps to attack any system

Conclusion

Ethical hacking must be used to fight against the black hat hackers and defend their attacks and protect every organisation from loss of data and secure their information and money. The main purpose of the research was to find an attack done using combining client-side and server side attacks.

Acknowledgement

I convey my gratitude to My Faculties for their valuable direction to write this paper, their suggestions, and comments. I pay my sincere thanks to my parents for their continuous support and encouragement.

References

- Manish Kumar, The Secret of Hacking 1st edition, 2009
- Srikanth Ramesh, Hacking Secrets Exposed, 1st edition, 2014
- Peter Van Eeckhoutte, Grey Hat Hacking The Ethical Hacking Handbook, 3rd Edition, 2011
- Chow, Ethical Hacking & Penetration Testing, 1st Edition, 2013

- Georgia Weidman, Penetration Testing a Hands on Introduction to Hacking, William Pollock, 1st edition
- Secure Planet LLC, The Hacker Playbook 2 Practical Guide To Penetration Testing, 2nd edition, Peter Kim, 2015
- Kathleen Wiso, Christopher Hadnagy, The Art of Human Hacking, 1st edition, 2015



Sohail Hussain is a Master of Computer Applications (MCA) from RV College of Engineering, Bangalore, Karnataka and keen in working in IT & Online Services.

sohailhussain5@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
10-Nov-2019	D62263938 (urkund)	1277	6845



Urkund Analysis Result

Analysed Document: 105-Research Materials-227-2-2-20200113.docx (D62263938)
Submitted: 10/11/2019 10:32:00
Submitted By: skesharwani@ignou.ac.in
Significance: 0 %

Sources included in the report:

Instances where selected sources appear: 0

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Disclaimer: All Views expressed in this paper are my own, which some of the content are taken from open source website for the knowledge purpose. Those some of i had mentioned above in references section.

Reviewers Comment

Reviewer Comment 1: Nowadays most references to hacking, and hackers, doing activity by cybercriminals—motivated by financial gain, protest, information taking, and even just for the “enjoy fun” of the challenge.

Reviewer Comment 2: The term computer “virus” originated to describe machine code command inserted into a computer’s memory that, on execution, copies itself into other programs.

Reviewer Comment 3: According to this article: Hacking is a technical in nature (like creating malvertising that deposits malware in a drive-by attack requiring no user interaction).

Editorial Excerpt

This article has 0% plagiarism which is accepted as per the standards of publication for the magazine. The author is in detail analyse the hacking in the various term according to definition “Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose “ Hence it is marked under “**Experiential Research Papers (ERP)**” category.



Scholastic Seed Inc.

www.scholasticseed.in

Citation

Sohail Hussain
“Hacking a Loophole in Computer Security”
Volume-1, Issue-6, Nov 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.