

Ethical Hacking

Prof Lavina Jadhav¹ Ms. Shafin Khan²

^{1,2}MET Institute of Computer Science, Mumbai, India

Abstract— Hacking and security is a fast moving sector of the computing industry and, as such, it is vital that one should be up to date with all the details about it. Also there is misconception among people that all hackers are bad. So in this paper there is description about hacking, its types, analysis on ethical hackers and security measures to be taken after system gets hacked with its benefits and drawbacks.

Key words: Hacking, Security

I. INTRODUCTION

Computer Hacking is a process to gain unauthorized access by manipulating systems resources But not all hackers are bad.



Fig. 1:

A. Who is a HACKER?

A hacker is an individual who uses his/her skills to exploit weakness in the computer system.

The following list classifies hackers according to their intent of hacking a system:

B. Mainly they are of 3 Types

1) White Hat Hacker

Also known as Ethical hacker. They never intend to harm the system rather they try to find out system's bugs or weakness.

2) Gray Hat Hacker

Combination of both white and black hat hackers.

3) Black Hat Hacker

They are known as crackers. They steal sensitive data by gaining unauthorized access.

II. FAMOUS HACKERS IN HISTORY

- 1) Kevin Mitnick
- 2) Jonathan James
- 3) Albert Gonzalez
- 4) Kevin Poulsen
- 5) Gary McKinnon
- 6) Robert Tappan Morris
- 7) Loyd Blankenship
- 8) Julian Assange
- 9) Guccifer 2.0
- 10) Anonymous

III. TYPES OF HACKING

- Website Hacking
- Email Hacking
- Network Hacking
- Password Hacking
- Computer Hacking
- Online Banking Hacking

IV. DIAGRAMMATIC FLOW

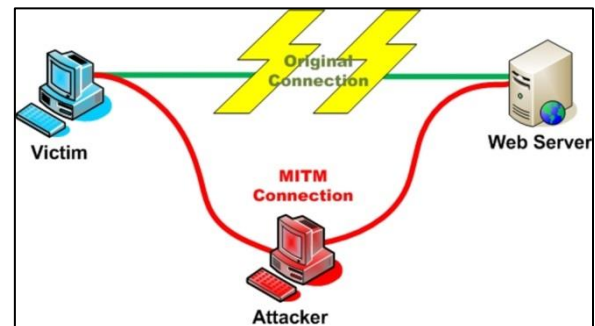


Fig. 2: Diagram Flow

V. ANALYSIS

IS HACKING NECESSARY?

YES... It's not just for Criminals Anymore

It is misconception that "ALL HACKERS ARE BAD"

Computer programmers called themselves hackers because they can break into the system and solves the problem. They can create a firewall to protect private data from being hacked.

According to an article in Whatis.com, hacking comes in different shapes and colors. Stating what kind of hacker he/she is.

Organizations such as HackThisSite.org promote Ethical Hacking. They offer training to any hackers who wants to learn to make environment safe.

A. Who Is Responsible For This Misconception?

Lack of awareness is the root cause among Common people. So let's see more about good hackers i.e. ETHICAL HACKING in detail.

VI. ETHICAL HACKING

- To test a security of the system against vulnerabilities with permission from the owner, ethical hackers report problems instead of taking advantage of them.
- Also known as penetration testing, intrusion testing and white hat.

A. What Does An Ethical Hacker Do?

- They use their programming skills to detect system's weakness and report the problem to higher authorities rather than taking advantage of the resources. Also their knowledge is used to protect system.

- Their main aim Security of the system and networks.

VII. FOLLOWING ARE THE TYPES OF ETHICAL HACKERS

- Hacktivists
- Cyber warrior
- Black Box Penetration Testers
- White Box Penetration Testers
- Certified Ethical Hacker/Licensed Penetration Tester

A. Phases

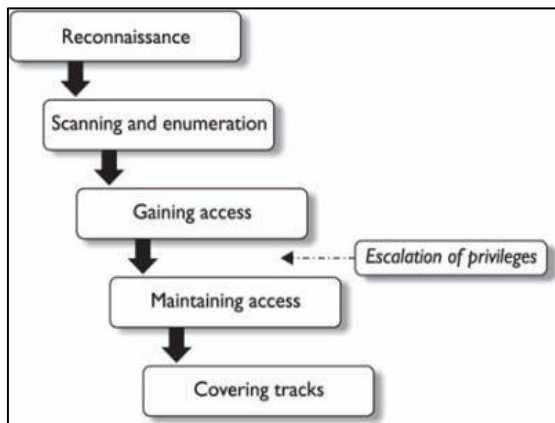


Fig. 3:

B. Need of Ethical Hacking

- To prevent the defense military.
- To prevent financial data from the high loss
- To protect the client's confidentiality.
- To validate risk assessment.
- Banker hire the ethical hackers for protecting the financial data.
- To create the security awareness at all levels
- To maintain the business functionality and confidentiality

VIII. EXAMPLES

- One of the earliest examples of using ethical hackers occurred in the 1970's. At this time, the United States government utilized the knowledge and services of groups of experts
- The United States Air Force used it to conduct a security evaluation of an operating system.
- The mom whose laptop was locked down by a ransomware attack.
- Tom was blackmailed because of his hacked Ashley Madison account.
- Hillary Clinton's Aides Got Phished And Lost Her The Election

IX. MEASURES TO PREVENT HACKING

- Stay Updated.
- Install a web firewall.
- Install security applications.
- Limit file uploads.
- Do not use open wifi.
- Use of strong passwords.

- Do not link accounts.
- Be careful with what you download.
- Turn off computer when not in use.
- Do not respond to fake email.

A. Benefits

- Fighting against terrorism and national security breaches.
- Having a computer system that prevents malicious hackers from gaining access.
- Having adequate preventative measures in place to prevent security breaches.
- Provide security to financial and banking sectors.

B. Drawbacks

- The ethical hacker using the knowledge they gain to do malicious hacking activities.
- Allowing the company's financial and banking details to be seen.
- The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system.
- Hiring professionals is costly.

X. CONCLUSION

- In this paper we have seen that Computer needs good security measure to prevent from hacking. So always be aware about online transactions and your activities and necessary steps related to computer usage like to turn off the internet when not in use and so on. Also keep watch on the site's protocol.
- One must use the technology as they are made for human convenience but use with precautions so that this technology will not land you into trouble.

REFERENCES

- [1] <https://www.makeuseof.com/tag/5-of-the-worlds-most-famous-hackers-what-happened-to-them/>
- [2] <http://hackersonlineclub.com/hackers-types/>
- [3] https://www.onlinebooksreview.com/uploads/blog_images/2018/01/20_31_hacking.jpg
- [4] <https://3c1703fe8d.site.internapcdn.net/newman/gfx/news/hires/2015/54edba5439d1f.jpg>
- [5] <https://www.hackthissite.org/articles/read/941>
- [6] https://www.google.co.in/search?q=security+life+cycle+of+hacking&rlz=1C1NHXL_enIN780IN780&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjNpsuiyvDZAhXEpY8KHSDLBDAQ_AUICigB&biw=1366&bih=637#imgdii=84IZ_rMzxiieZM:&imgsrc=jbZIFvdP1t3lMM
- [7] <https://heimdalsecurity.com/blog/12-true-stories-that-will-make-you-care-about-cyber-security/>