WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Ethical Hacking & Hacking Attack with Prevention

Satish Kumar, Laxminarayan Mishra

Department of Computer Application, IMCOST Collage Thane, University of Mumbai, 400068

DOI: https://doi.org/10.55248/gengpi.2022.3.6.51

ABSTRACT:

In this Digital Era our all information is available online on our social media, now day huge number of user using social media platforms and this information is used by someone to get knowledge but some of them use this information to destroy or steal without our knowledge this above line is a part of hacking and who does so called HACKER if there is any bad happen the savior will and our savior is ETHICAL HACKER who save us to form these type of actions need of them.

Key Words: What is Ethical Hacking, Information about Hacker Dos, Phishing, etc. Prevention from Hacking

1. INTRODUCTION

From the year 1980's, the Internet was vastly grown in public and computer security has become a major concern for businesses and governments. Organizations would like to use the Internet to their advantage by utilizing the Internet as a medium for e-commerce, advertising, information distribution and access, as well as other endeavors. However, they remain worried that they may be hacked which could lead to a loss of control of private and personal information regarding the organization, its employees, and its clients.

In way to finding ways to reduce the fear and worry of to be hacked, organizations have come to the realization that an effective way to evaluate security threats is to have independent security analyst attempt to hack into their computer systems. In the case of computer security, these *teams* or *Ethical Hackers* would use the same tools and techniques as an attacker, but rather than damage the system or steal information, they would evaluate the system security and report the risk they found and provide instructions for how to put right them.

2. Information About

Ethical hacker is work to investigate the system and network to find weak points that hacker will going to destroy. They collect and analyze the information to figure out way to strengthen the security of the application. This practice helps to identify security vulnerabilities which then be resolved before a malicious attacker has the opportunity to exploit them.

There are main Three Type of Hacker

1.White Hat Hacker

2 Black Hat Hacker

3 Grey Hat hacker

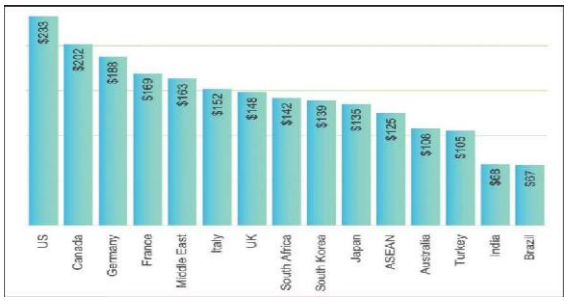


Table -1:Shows How much money Protected by Ethical Hacker

White Hat Hacker

The good guys! White hat hackers are cyber security experts and geniuses who are officially employed by corporations to keep their network safe and secure from any type of breaches. They search the network for any loopholes or any vulnerabilities that can be exploited by Black Hat hackers,

resulting in loss of up to millions of dollars at a time. If and when one's network is attacked, they are the ones who come to the rescue by trying to minimize damage that being done by a malicious attack.

Black Hat Hacker

The bad guys! These are the hackers that are pictured in the many movies. They consider themselves above the law and are hence, always on the lookout for vulnerabilities in corporate and banking networks. They do so for selfish financial gains and also for malicious intent when they try to hack in to operations dealing with national security and safety. They often upload ransomware and malware onto networks hoping to exploit any vulnerability or loophole that hasn't been detected by the White hat hackers.

Grey Hat Hacker

These Guys Are Ethical Hacker Plus Cyber Criminal

The **Good & Bad both**! Just like there is no black and white in life, similarly in the hacker community, the color grey brings about a sense of balance. They can either hack in to networks and cause losses or be employed by the same and work in a manner similar to that of white hat hackers. The fine line of difference between the White hat and grey hat hacker is that the white hat finds network vulnerabilities privately while the grey hat does it publicly.

Apart from these

Red Hat: Red hat hacker is also a good guys in cyber world they work as white hat hacker but they only target Linux based system they take an aggressive step to stop Black Hat hackers, they do everything to stop bad guys in Cyber World else they also taking matter into their own hands.

Green hat: These hackers are not aware of the security mechanism and the inner workings of the web, but they are keen learners and determined (and even desperate) to elevate their position in the hacker community.

Blue Hat: Blue Hat hacker is different type of hacker who works out side of the organization they are security expert work in companies to test the new software and finding bugs. Microsoft is well known for hiring these hackers to test their software.

These are some name of Attack what is done by Hacker

- **Password sniffing**
- **Denial of service(DoS)**
- **Trojan Horse**
- **Virus**
- **Email bombing**
- **Phishing Attack**

Password Sniffing

It is an attack use to steal any people's user name and password from their network, it is also called data theft it occurs when someone capturing network traffic through packet sniffer.

Denial of service(DoS)

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. It is a cyber-attack its purpose to make a machine or network resource unavailable.

Virus

It is a type of malicious software or it is malware, as per its behavior it spared, it is spread through computers and cause damage to our data and software and the result in data loss and leakage.

Email Bombing

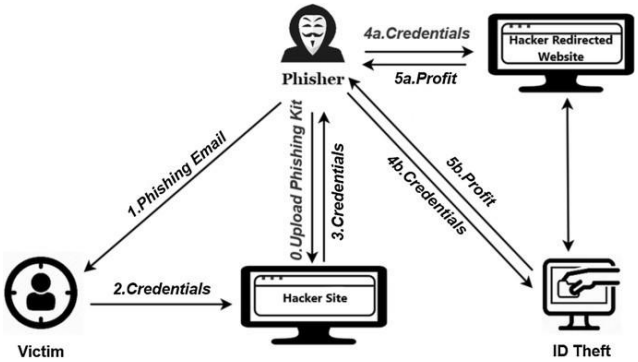
Refers to sending large number of emails to the victim to crash victim email account.

Trojan Horse

It is a type of malware, it occurs due to lack of security knowledge of the user and security measure on a computer. It is often appears as a malware attachment through our email or any social media and comes from trusted source.

Phishing Attack

They will use these and go out into the public somewhere and make a connection available that you can connect with wirelessly. Usually they will connect with a legitimate wireless connection that is available in the public are and as kit



Ex- With the help of this link we can see required things of victim by just clicking once like IP address, current location etc.
https://iplogger.org/

Prevention from Hacking

Computer virus and hacking attacks can damage your PC, send sensitive data toattackers, and cause downtime until the system is repaired.You can avoid becoming the next computer virus victim byfollowingafewbestpractices

Install AntivirusSoftware:

Antivirus software is first thing what defend against any malicious virus and provide firewall safety to prevent hacker away from our network but this is not permanent solution that can help not be hacked it just little step that can help to be safer in cyber world.

Don't open executable email attachments:

Numerous malware attacks including ransomware start with a vicious dispatch attachment. Executable attachments should never be opened, and druggies should avoid running macros programmed into lines similar as Microsoft Word or Excel. Keep your operating system updated.

Inventors for all major operating systems release patches to remediate common bugs and security vulnerabilities..Alwayskeepyouroperatingsystemupdated and stop using end-of-life versions (e.g., Windows 10+ orWindowsXP)

Avoid Questionable Websites

Aged cyber surfers are vulnerable to exploits used when just browsing a website. You should always keep your cyber surfer streamlined with the rearmost patches, but avoiding these spots will stop drive- by downloads or turning you to spots that host malware.

Don't use pirated software

Free appropriated software might be tempting, but it's frequently packaged with malware. Download seller software only from the sanctioned source and avoid using software that's appropriated and participated.

Conclusion:

The whole world is moving towards the enhancement of technology, and more and more digitization of the real world processes, with this the trouble of security increases. This paper described the working of vicious hackers or crackers on one hand who tries to immorally break into the security and on the other hand white headpiece hackers or ethical hackers, who tries to maintain the security. As in the computer system, playing plays a vital part as it deals with both sides of being good or bad. Further, this paper tells about the types, working, and various attacks performed by the hackers. In conclusion, it must be said that Ethical Hacking is a tool which when properly employed can help in better understanding of the computer systems and perfecting the security ways as well.

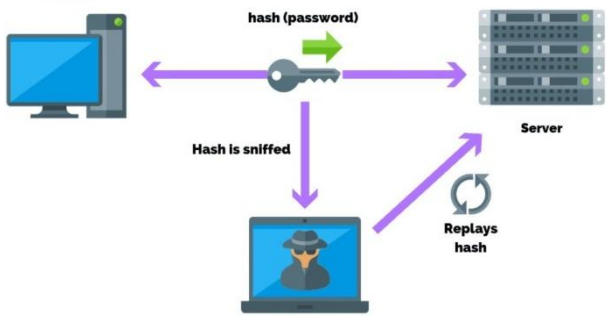


Fig3.Way to Protect your self-form hacking

REFERENCE

Hawamleh, A.M.A., Alorfi, A.S.M., Al-Gasawneh, J.A. and Al-Rawashdeh, G., 2020. Cyber security and ethical hacking: The importance of protecting user data. Solid State Technology, 63(5), pp.7894-7899.

Berger, Hilary, and Andrew Jones. "Cyber security & ethical hacking for SMEs." In *Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society*, pp. 1-6. 2016.