International Journal of Research Publication and Reviews

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

ETHICAL HACKING AND HACKING ATTACKS

Jigar Vijay Chheda[1]*, Asst. Prof. Gauri Ansurkar*[2]

[1,2]*Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India, chhedajigar123@gmail.com*

ABSTRACT

As nowadays all the information is available online, a large number of users are accessing it, some of them use this information for gaining knowledge and some use it to know how to use this information to destroy or steal the data of websites or databases without the knowledge of the owner. The purpose of this paper is to tell what is hacking, who are hackers, what is ethical hacking, what is the code of conduct of ethicalhackers and the need of them. A small introduction of Linux Operating System is given in this paper. All the techniques are performed on the Linux operating system named Kali Linux. After this some basic hacking attacks covered in the paper are MiTM Attack (Man in The Middle Attack), Phishing Attack, DoS Attack (Denial of Services Attack). Further what is Wi-Fi, what are the techniques used in the Wi-Fi protection and the methods used by the hackers to hacks Wi-Fi passwords is covered in the paper.

Keywords*: Hackers, Ethical Hackers, MiTM, DoS, Phishing, Wi-Fi phishing, Code of conduct*

1. INTRODUCTION

As a computer technology advances, it has its darker side also; HACKERS. In today world the size of the internet is growing at a very fast rate, a large amount of data is moving online, therefore, data security is the major issue. The internet has led to the increase in the digitization of various processes like banking, online transaction, online money transfer, online sending and receiving of various forms of data, thus increasing therisk of the data security.

Ethical hacking technology spreads to diverse areas of life and in particular to every walks ofthe computer industry. The required to protect dominant data of the common should be communicate with the correct technology. Nowadays a large number of companies, organizations, banks, and websites are targeted by the various types of hacking attacks by the hackers. Generally, after hearing the term hacker we all think of the bad guys who are computers experts with bad intensions, who tries to steal, leak or destroy someone's confidential or valuable data without their knowledge. They are the persons with very high computer skills who tries to break into someone else security for gaining access to their personal information, but all the times it is not like that. To overcome the risk of being hacked by the hackers we have Ethical Hackers in the industry, who are also computer experts just like the hackers but with good intensions or bounded by some set of rule and regulations by the various organizations.

A. WHAT IS HACKING?

Ethical hacking technology spreads to diverse areas of life and in particular to every walks of the computer industry. The required to protect dominant data of the common should be communicate with the correct technology. Hacking is the technique of finding the weak links or loopholes in the computer systems or the networks and exploiting it to gain unauthorized access to data or to change the features of the target computer systems or the networks. Hacking describes the modification in the computer hardware, software or the networks to accomplish certain goals which are not aligned with the user goals. Ethical hacking becoming a powerful policy in fighting online threats with the rise of cybercrime. In contrast, it is also called breaking into someone's security and stealing their personal or secret data such as phone numbers, credit card details, address, online banking passwords etc.

HACKERS

The team HACKER in the popular media is used to describe someone who breaks in to someone else security using bugs and exploits knowledge to act productivity or maliciously. The ethical hacker search ports, websites & locate bugs that can be targeted by a cracker. Once the weaknesses for any device are known, the attacks can be done easily. Hackers are the computer export in both hardware as well as software. A hacker is a computer enthusiast and master in a He is kind of person who loves to learn various technologies, details of the computer system and enhances his capability and skills.

TYPE OF HACKERS

Hackers can be classified into Three main groups.

A. White Hat Hackers.

B. Black Hat Hackers.

C. Grey Hat Hackers.

A. <u>WHITE HAT HACKERS</u>

A white-hat hacker, also known as the ethical hackers. White Hat Hackers use their skills and knowledge to protect the organization before malicious or bad hackers find it and make any harm to the company or the organization. It is celebrity who has non-mischievous intent every time they breaks into security systems. Most white-hat hacker is safety specialist, often working with a company to track & enhance security weaknesses legally. White hat hackers are the authorized persons in the industry, although the methods used by them are similar to those of bad hackers but they have permission from the organization or the company who hires them to do so.

B. <u>BLACK HAT HACKERS</u>

The ' black-hat ' hackers, sometimes referred to as a ' cracker, ' is a computer hardware and software expert who breaks intothe security of someone with malicious intent and without permission. The hackers typically want to prove her or his hacking skills & will perform a variety of cybercrimes, such as credit card fraud, identity theft and piracy and damaging their important or secret information.shutting down or altering functions of websites and networks. A black hat hacker is a person with detailed computer knowledge aimed at infringing or bypassing internet security. They violate the computer security for their personal gain.

C. <u>GREY HAT HACKERS</u>

As the color suggests, somewhere between white-hat & black-hat hackers is a ' grey-hat 'hacker, as he or she possesses both characteristics. A Grey Hat Hacker is a computer hacker or security expert who sometimes violates the laws but does not have any malicious intentions like the black hat hackers. The term Grey Hat is derived from the Black Hat and the White Hat as the white hat hackers finds the vulnerabilities in the computer system or the networks and does not tells anybody until it is being fixed, while on the other hand the black hat hackers illegally For example, in search of compromised systems, some grey-hat hackers will roam in the Internet; like the white-hat hackers, the targeted company will be aware of any vulnerability & will patch them, but like the grey-hat hacker, the black-hat hacker will hack without permission. Exploits the computer system or network to find vulnerabilities and tells others how to do so whereas the grey hat hacker neither illegally exploits it nor tells anybody how to do so.

D. <u>BLUE HAT HACKERS</u>

Independent specialist companies for computer security are employed to check a program for vulnerabilities before it is released, finding weak links that can be removed. Blue hat is also affiliated with Microsoft's annual security convention where Microsoft engineers & hackers are able to communicate freely. Blue hat hackers are someone outside of the consultancy firm of computer security who tests a system before it is launched, looking for exploits to be closed.

E. <u>ELITE HACKERS</u>

These type of hackers that have prominence as the ' best in the business ' & are regarded as the innovators & experts. The invented language called ' Leets peak' was used by elite hackers to shield their pages from searching engines. A language meant that few letters were replaced in a words by the numerical similarity or other similar letters.

2. ETHICAL HACKING PROCESS:

Ethical hacking is learning the conception of hacking and applying them to secure any systems, organization for any great cause. FIG. describes the level for ethical hacking consisting of five blocks.

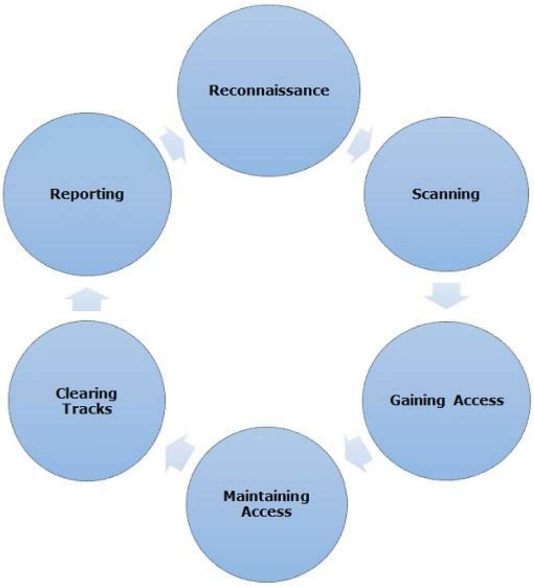
A. Reconnaissance.

B. Maintaining Access

C. Scanning & Enumeration

D. Gaining Access

E. Clearing Tracks



Ethical Hacking Steps

A. RECONNAISSANCE

The process of collecting information about the target system is called reconnaissance. It is the set of procedures & technique used to gather information's about the target systems secretly. In this, the ethical hacker seeks to gather as more information as possible about the target systems, following the 7 steps mentioned below.

a) Identification of active machines

b) Preliminary information collection

c) Identification of every ports services

d) Network mapping

e) Identification of open ports & access points

f) OS fingerprinting

B) SCANNING

The 2nd step of the penetration testing & ethical hacking is the enumeration and scanning. Scanning is the common technique that pen tester uses to find the open door. Scanning is worn to determine the weaknesses of the service that operate on the port. They need to figure out the operating systems included, live host, firewalls, services, intrusion detection, perimeterequipment, routing & general networks topology (physical network layout) that are parts of thetargets organization during this phase. Enumeration is the main priority network attack. Enumeration is a producer by actively connecting to it to collect information about the target.

C) GAINING ACCESS

Once the observation is finished & every weakness are tested, the hackers then attemptswith the helps of some tools & techniques to gain access. This essentially focuses on theretrieval of the password. Either bypass techniques or password cracking the techniques that can be used for this by hacker.

D) MAINTAINING ACCESS

Once the intruder has got access to the targeted systems, he can take advantage of both thesystems & its resources & use the systems as a catapult pad for testing & harming other system,or can retain the low profile & continue to exploit the systems without the genuine user knowing every acts. Those 2 acts will demolish the organization that leads to a calamity. Rootkits gain entrance at the operating systems level, while the Trojan horses gain entrance at the program levels. Attackers that can use the Trojan horses to migrate on the system user passwords, names & credit card information's.Organizations that can use tools for honeypots or intrusion detection to detect the intruders. Nonetheless, the hindmost is not commend unless the company has the necessary security personnel to take advantage of the defense principle.

E) CLEARING TRACKS

For several purposes such as avoiding detection & further penalizing for intrusion, an offender will destroy confirmation of his activities and existence. Eliminating evidence that is often referred to the ' clearing tracks ' is the requirement for every intruder who needs to remain anonymous and prevent detect back. Usually this steps begins by delete the adulterate logins or all other possible errors messages generated from the attack process on the victim system. For e.g., a buffer overflow attack usually leaves a message that needs to be cleared in the systems logs. Next attention is focused on making changes in order not to log in to potential logins. The 1st thing a systems administrator does to trace the system'suncommon activity is to review allthe systems log file, it is necessary for trespasser to use the tool to change the system logs sothat the administrator cannot track them. Making the system look like it did before they obtainaccess & set up backdoor for their own use is important for attackers. Any files that have beenmodified must be swap back to their actual feature's so there is no doubt into the mind ofadministrators that the systems have been trespasser.

TOOLS USED IN ETHICAL HACKING

- **Tools for Reconnaissance:** Google, Whois Lookup and NSLookup**.**
- **Tools for Scanning:** Ping, Tracert,Nmap, Zenmap, NiktoWebsiteVulnerability Scanner, Netcraft.
- **Tools for Gaining Access**: John the Ripper, Wireshark, KonBoot, pwdump7, Aircrack, Fluxion, Cain and Abel.
- **Tools that are used for the Maintaining Access**: Metasploit Penetration Testing Software, Beast, Cain & Abel.
- **Tools for Clearing Tracks***:* Metasploit Penetration Testing Software, OS Forensics.

THE CODE OF CONDUCT OF AN ETHICAL HACKER

- Identifying and determining the confidentiality and privacy of the data of any organization beforehacking and should not violate any rule and regulations.
- Before and after the hacking maintaining the transparency with the client or owner of the organization.
- The intensions of an ethical hacker must be very clear, that not to harm the client or organization.
- Working within the limits set by the client or the organization, do not go beyond them.
- After the hacking do not disclose the private or confidential findings during the hacking with others.

NEED OF ETHICAL HACKERS IN THE INDUSTRY

As every organization has its own confidential information which can be hacked by the malicious hackers or can be damaged by them therefore in order to protect that information the organizations heir ethical hackers and allow them to hack their own systems ethically any Now starting with some hacking attacks performed by the hackers over the internet with the help of linux system.

Linux operating system just like the windows and Mac. An operating system is an interface between the user and the computer hardware.

Unlike Microsoft Windows and Mac operating systems the Linux are the open source operating systems as it is distributed under open source license. It is more secure than the windows and has very less number of viruses known which will harm Linux OS.

Further in this paper the attacks are performed on the Kali Linux Operating System. Kali Linux Operating system is a Linux distribution which is mainly used for penetration testing and security auditing. Kali Linux contains various tools for computer forensics, penetration testing, reverse engineering etc. Kali Linux is developed by "Offensive Security".

The kali Linux Security Attack like

1. Phishing
2. Denial of Services (DOS)
3. Man in the middle attack
4. Wi-Fi

TARGETED SYSTEMS

The new adaptation and the widespread use of the internet was based on the digitize of written data and records intodigital data and information stored in the cloud services. This led hackers to finding it as a great way to lead their cyber-attacks against various yet numerous targets.

a) Banks

b) Enterprises

c) Governments

d) Hospitals

e) Individuals

f) Military Website

g) Big Organization

SECURITY, SAFETY PROCEDUR

Despite the different preventive and protective security measures being recommended, many steps need to be considered to ensure both security and safety measures. Incident responders must be distinguished and classified to maintain the right response against any given event(s). Once achieved, preventive and protective security measures must be employed for further protection.

Security & Safety Procedures Steps:-

The focus should also be based on ensuring security and safety procedures that each employee must follow and adhere to. In fact, it can only be achieved by relying on continuous, consecutive and constant training and awareness, including

- Step 1: employees must not use Free Wi-Fi to log in, nor rely on public computers so their credentials are not stolen. Additionally, changing passwords regularly also helps. It is also important to know which site is being visited through the “secure sign” and “Hyper Text Transfer Protocol Secure” (HTTPS) instead of “HTTP”.

- Step 2: the browser’s history must be cleared to prevent any attacker from conducting a cookie theft or/and masquerading attacks without the user’s knowledge. Moreover, it is also important to know what link to click on, simply by avoiding spam email based on phishing attack types.

- Step 3: IT staff must be trained as emergency response and disaster recovery teams in case of any possible attack taking place. Therefore, being able to assess the likelihood and impact of a given risk based on the threat of exploiting a given vulnerability.

- Step 4: the company’s paper waste must be eliminated by destroying every piece of paper, disk, or hardware component beyond recovery and recognition, so that the thrown garbage cannot be used as an information gathering method to know the company’s little secrets. This can also be achieved if the organization follows paperless processes.

- Step 5: strong identification and authentication mechanisms can be used if they rely on biometric procedures to access sensitive locations in a given organization, through additional extensive security procedures. Moreover, employees must lock their devices after leaving for a break or home, and lock their desks to prevent any confidential paper leakage. Therefore, no device should be left unattended.

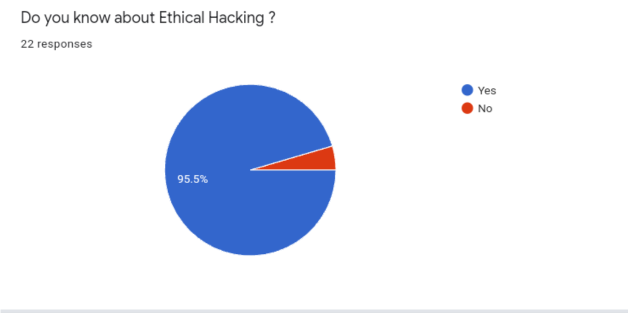
- Step 6: employees must be trained against different social engineering, and phishing attack techniques and types. This can be done by limiting the information given on a given phone, or through face-to-face chatting, or even through instant messaging. This also includes how to identify phishing attacks based on sending fake infected CV formats or sending malicious links, or war-dialing..

- Step 7: employees must be trained in their own domains against various cyber-attack types, but mainly against insider attacks. Moreover, employees must be prevented from using USBs, in addition to their own devices.

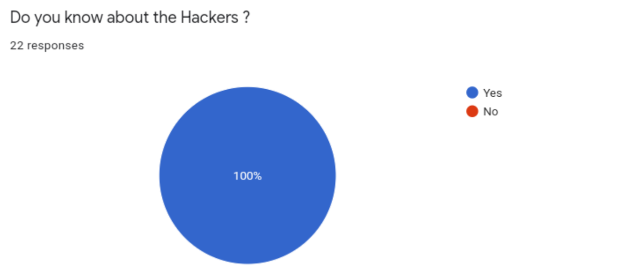
- Step 8: Previous employees should have all their forms of access controls, rights and privileges to the system removed. This includes their previous IDs, access privileges, passwords, e-mails, biometrics and cards.

PUBLIC SURVEY

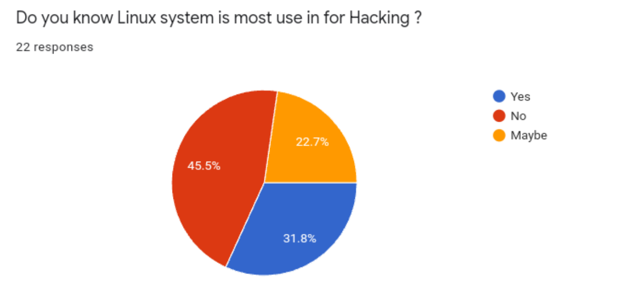
Figures and Survey Results


Do you know about Ethical Hacking ?

22 responses


Do you know about the Hackers ?

22 responses


Do you know Linux system is most use in for Hacking ?

22 responses

3. CONCLUSION

The whole world is moving towards the enhancement of technology, and more and more digitization of the real world processes, with this the risk of security increases. This paper described the working of malicious hackers or crackers. Proper security will not be a fact as long as there is funding for ad-hoc & security solutions for these insufficient designs & as long as the delusory results of intrusion team are recognized as evidence of computer systemssecurity. Regular monitoring, attentive detection of intrusion, good systems management practice & awareness of computer security that all essential components of the security effort of an organization.As in the computer system, hacking plays a vital role 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 utilized can help in better understanding of the computer systems and improving the security techniques as well.

ACKNOWLEGMENT

It gives me great pleasure to present my Research paper on “Ethical Hacking and Hacking Attacks”. I would like to express my sincere thanks to all the teachers who helped us throughout. I would like to acknowledge the help and guidance provided by our professors in all place during the presentation of this research paper. We are also grateful to, Head of Department. This acknowledgement will remain incomplete if we do not mention sense of gratitude towards our esteemed Principal who provided us with the necessary guidance, encouragement and all the facility available to work on this project.

REFERENCES

[1] [https://www.google.com

[2] [Figure and chart