A REVIEW ON ETHICAL HACKING

1stAman Vikas Dakhare
dakhareaman74@gmail.com
Department of Computer Science
And Engineering
Shri Sai College of Engineering and
Technology,Chandrapur ,India

2nd Prof Vijay Rakhade
vijayrakhade@gmail.com
Department of Computer Science
And Engineering
Shri Sai College of Engineering and
Technology,Chandrapur ,India

3rd Prof Lowlesh Yadav
lowlesh.yadav@gmail.com
Department of Computer Science
And Engineering
Shri Sai College of Engineering and
Technology,Chandrapur ,India

ABSTRACT:

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.It is also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use,but with one major difference that Ethical hacking is legal. hacking Inform hardware and software vendors of the identified weaknesses Transparently report - All the identified weaknesses in the computer system to the organization Protect the privacy of the organization been hacked. Ethical hacking is testing the resources for a good cause and for the betterment of technology ◦ It also means to secure the system. ◦ There is a tremendous rise in cybercrimes, so in those cases ethical hacking act as a safeguard on internet and corporate networks and their websites.

Keywords: Ethical Hacking, Types of Hacking, Phases of Ethical Hacking.

INTRODUCTION:

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating the strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.Four key protocol concepts followed by Hacking Experts:

Stay legal. Obtain proper approval before accessing and performing a security assessment.

Define the scope. Determine the scope of the assessment so that the ethical hacker’s work remains legal and within the organization’s approved boundaries.

Report vulnerabilities. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.

Respect data sensitivity. Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

Fig No.1 Ethical Hacking

Types of Hackers

A hacker is a person who solves a technical issue by using a computer, networking, or even other abilities. Anyone who uses their skills to gain access to a system or network in application to break laws is referred to as a hacker.

White Hat Hackers

On the dark, these are the right people who come to our aid. White hat hackers, also known as ethical hackers, are cybersecurity experts who assist the government and identifying security flaws. Ethical hackers use a variety of techniques to protect themselves from black hat hackers and other cybercriminals. They break into our system with the good intention of finding vulnerabilities and assisting you in removing viruses and malware.

Black Hat Hackers

These days, black hat hackers the majority of the timeis monetary. These hackers look for flaws in individual computers in businesses and banking systems. They can hack into your network and gain access to your personal, business, and financial information by exploiting any loopholes they find.

Grey Hat Hackers

Grey Hat Hackers fall in between white and black hat hackers. Grey hat hackers may not use their skills for personal gain, they can however have both good and bad intentions.

Fig No.2 Types of Ethical Hacking

Phases:

Reconnaissance/Footprinting

Reconnaissance is the first phase of ethical hacking, also known as the footprinting and information gathering phase. This is the preliminary phase where white hat hackers gather as much information as possible and implement security measures into the targeted system or network. The information gathered by white hat hackers usually is about three groups: network, host, and people. There are mainly two types of footprinting:**Active footprinting and Passive footprinting.**

Scanning

The scanning phase is the second step in an ethical hacker's methodology. It entails applying all the knowledge learned during the reconnaissance phase to the target location to search for vulnerabilities. Hackers search for data such as user accounts, credentials, IP addresses, etc. There are three types of scanning, which include:**Port scanning, Vulnerability scanning, Network Scanning**

Gaining : In this phase, the hacker creates the blueprint for the target's network using the data gathered in Phases 1 and 2. The hacker obtains access to the network, programs, and system and then extends their access permissions to manage connected systems.

Maintaining: When a hacker gains access, they choose to maintain it for future exploitation and attack. In addition, the hacker gains access to the organization's Rootkits and Trojans and utilizes them to execute more network attacks. An ethical hacker attempts to keep access to the target until they have completed the activities or intend to complete in that target.

Clearing Tracks:Once a hacker has obtained access, they leave no trace to prevent detection by the security team. They execute this by deleting cache and cookies, interfering with log files, and closing all open ports. This incorporates some of the steps an ethical hacker uses to cover and eliminate their footprint.

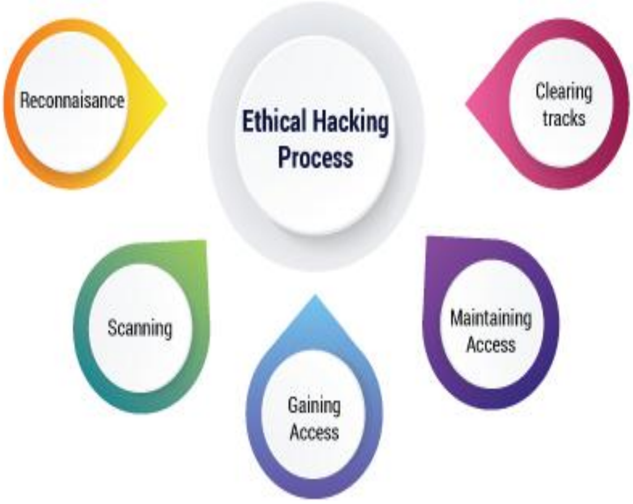

Fig No.3 Phases of Ethical Hacking

Advantages of Hacking :

- To improve lost information, specifically in case if you lost your password.

- To implement penetration testing to fortify computer and network security.
- To put satisfactory preventative methods in place to prevent security breaches.
- To have a computer system that avoids malicious hackers from gaining access.

Disadvantages of Hacking :

If Hacking is done with the destructive intent, then it could be dangerous. It can effect

- Enormous security fissure.
- Unauthorized system access on the private/secretive information.
- Privacy destruction.
- Fettering system operation.
- Denial of service attacks.
- Malicious attack on the system/network.

CONCLUSIONThe security problems will endure as long as constructor remain committed to present systems architectures, generated without some security requirements. 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 systems security. 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. In any of these places, a single failure could well expose a company to cyber vandalism, loss of revenue, humiliation or even worse. Each new technology has its advantages & risks. While the ethical hackers that can help customers better appreciate their security needs, keeping their guards in place is up to customers.

REFERENCES:

[1]Prabhat Kumar Sahu, Biswamohan,” REVIEW PAPER ON ETHICAL HACKING” International Journal of Advanced Research in Engineering and Technology (IJARET) Volume 11, Issue 12, December 2020, pp. 163-168, Article ID: IJARET_11_12_018

[2] Sushil Bhardwaj,” Review on Teaching Ethical Hacking” International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-10, Issue-2, Mar 2022

[3]Ms. Vaishnavi Bhagwat Savant ,” A REVIEW ON OVERVIEW OF ETHICAL HACKING “International Journal of Engineering Applied Sciences and Technology, 2021 Vol. 6, Issue 4, ISSN No. 2455-2143, Pages 379-383 Published Online August 2021 inIJEAST

[4]Shubham Apteka1 ,NeharaniBaital , “Ethical Hacking Techniques”,International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VI June 2022

[5] Fiza Abdul Hafiz Qureshi, Mayur Dube, Komal Ramteke, Akshay Akhare “A Review Paper on Ethical Hacking”,International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal Volume 3, Issue 1, August 2023

[6] Ishan Ahuja1, Suniti Purbey2, “REVIEW PAPER ON ETHICAL HACKING” International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 08 Issue: 04 | Apr 2021

[7] Jigar Vijay Chheda1 , Asst. Prof. Gauri Ansurkar2, “ETHICAL HACKING AND HACKING ATTACKS”International Journal of Research Publication and Reviews Journal homepage: www.ijrpr.com ISSN 2582-7421

[8] Ms. Priyanka Bhardwaj ,Ms. Preeti , “A Review on Ethical Hacking”International Journal of Advanced Science and Technology

[9] Vinitha K. P, “Ethical Hacking “ International Journal of Engineering Research and Technology(IJERT)

[10] Lowlesh Nand kishor Yadav, “Predictive Acknowledgement using TRE system to reduce cost and Bandwidth”, IJRECE VOL7 ISSUE 1(January-march 2019)