IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

Exploring Ethical Hacking: Tools, Techniques, and Defensive Strategies

Shital Dilip Jadhav
MCA Student
Institute of Distance and Open Learning, Mumbai, Maharashtra, India
shitaljadhavckt31@gmail.com

Abstract: *The rising prominence of ethical hacking, commonly referred to as penetration testing, has emerged as a significant issue for both businesses and governments. The prospect of being targeted by malicious hackers is a constant worry for companies, while individuals are increasingly concerned about safeguarding their personal information. This article delves into the world of ethical hackers, exploring their expertise, the diverse range of tools they employ, different types of attacks they simulate, and the methods they employ to assist their clients in identifying and rectifying security vulnerabilities. Undoubtedly, this process presents numerous challenges that need to be overcome*

Keywords: Hacking Techniques, hackers approach, call spoofing attack, brute force attack, Bomber, pen testing, MetaSploit

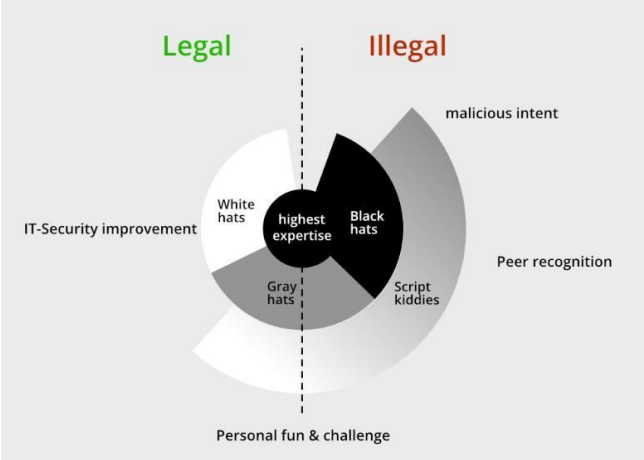
I. INTRODUCTION

In the IT industry today, there exist various terms to de- scribe individuals involved in hacking activities. As the Internet continues to expand, security has become a major concern for both businesses and government bodies. The widespread desire to utilize the Internet for e-commerce, information distribution, and accessing various luxuries and necessities is accompanied by the paramount concern of protecting personal information, including bank details, home addresses, and other sensitive data
[1]. This growing need for security gave rise to the term ”Ethi- cal Hacking.” Organizations and government bodies recognized that one of the most effective ways to counter intruders and po- tential threats was to employ hackers who could assess their systems or databases without causing damage, manipulation, or data theft. Instead, these ethical hackers would identify vulner- abilities and provide detailed reports to the owner, along with instructions on how to patch those vulnerabilities. Therefore, these hackers came to be known as ”Ethical Hackers.” Before engaging in their work, ethical hackers typically sign written contracts with the owners, granting them permission to access their systems and search for vulnerabilities. In general, there are three main types of hackers.

- WHITE HAT
- BLACK HAT
- GREY HAT

In the realm of hacking, there are different categories of hack- ers based on their intentions and actions. White hat hackers, also known as ethical hackers, refrain from utilizingtheir skills for personal gain unless contracted to identify vulnerabilities in specific systems or databases. Their primary purpose is to pro- vide protection against black hat hackers, who are the actual intruders driven by malicious intentions. Ethical hackers are hired to safeguard systems from these black hat hackers. One important aspect they prioritize is maintaining their anonymity.
The term ”grey hat hackers” refers to individuals who ex- hibit characteristics of both black hat and white hat hackers. They possess malicious intentions but also offer security ser-vices. However, once they engage in protecting a system, they do not attempt to manipulate it. The term ”grey” signifies the blending of the black and white hat hacker characteristics.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024



II. LITERATURE REVIEW

Techniques of ethical hacking:

- Information gathering
- Vulnerability Scanning
- Exploitation
- Test Analysis

Information gathering: During the initial phase of penetration testing, known as test analysis and information gathering, the tester focuses on gathering as much information as possible about the target. The effectiveness of the penetration test largely depends on the tester's in-depth understanding of the target [8]. The tester collects all available information, even though it may initially appear irrelevant, as the specific information needed for the test is unknown. This step can be carried out using various public tools, including search engines, scanners, and by sending simple HTTP requests. Additionally, the tester may also rely on interacting with the application itself to gather necessary data for the assessment.

Vulnerability Scanning: Once the testers have gathered the necessary information, they can proceed to conduct testing on various aspects of the target application. These include configuration management, business logic, authentication, session management, authorization, data validation, denial of service, and web services [8]. Leveraging the knowledge obtained during the information gathering step, the testers then scan for vulnerabilities that may exist within the application. This involves examining vulnerabilities related to authenti- cation mechanisms, input validation, and function- specific vulnerabilities. By thoroughly assessing these areas, the testers aim to identify potential weaknesses that could be exploited by malicious actors.

Exploitation: After completing the vulnerability analysis step, the ethical hackers or testers gain a thorough understanding of the areas that are susceptible to exploitation. This knowledge allows them to determine the specific targets for conducting exploits. The exploitation step involves the use of various tools and methods to actively exploit the identified vulnerabilities.

The choice of tools and methods for exploitation can vary depending on the nature of the vulnerabilities and the systems being tested. Some common tools and techniques used in this phase include:

Exploit Frameworks: Ethical hackers utilize exploit frame- works such as Metasploit, Core Impact, or Canvas. These frameworks provide a collection of pre-built exploits and at- tack vectors that can be used to exploit known vulnerabilities in target systems.

Custom Scripts: Ethical hackers may develop their own cus- tom scripts or tools to exploit specific vulnerabilities or target unique system configurations.

Payloads: Attackers often use payloads, such as command shells, reverse shells, or malicious code, to gain unauthorized access, execute arbitrary commands, or establish a persistent presence within the target system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

Social Engineering Techniques: In some cases, ethical hack- ers may employ social engineering techniques to exploit human vulnerabilities and gain unauthorized access to systems. This could involve phishing attacks, impersonation, or other manip- ulative tactics to deceive users and extract sensitive information. The exploitation phase is a critical part of the ethical hacking process, as it helps identify the potentialimpact and severity of the vulnerabilities discovered during the assessment. However, it's important to conduct exploitation only within the authorized scope and with proper permissions to ensure the security and integrity of the systems being tested.

Test Analysis Phase: The Test Analysis Phase serves as the fi- nal stage of the ethical hacking process. It acts as the interface between the assessment results and the target system. During this phase, any vulnerabilities discovered in the system are re- ported back to the owner or client who hired the ethical hacker. The primary objective is to provide the necessary information and recommendations to improve the security of the system.

In this phase, the ethical hacker prepares a comprehensive report detailing the vulnerabilities identified during the assessment. The report includes a description of each vulnerability, its potential impact, and any supporting evidence. Additionally, the report may contain recommendations for mitigating the vulnerabilities and improving the overall security posture of the system.

The patches or fixes necessary to address the identified vul- nerabilities are also provided to the owner or hirer.These patches may include software updates, configuration changes, or other specific measures tailored to address the vulnerabilities in the system.

Ultimately, the Test Analysis Phase plays a critical role in bridging the gap between the assessment results and the target system's security. It enables the owner or hirer to take appro- priate actions based on the identified vulnerabilities and recommendations to enhance the system's security and protect it from potential threats.

III. METHODOLOGY

The primary approach of owners is to obtain an evaluationfrom ethical hackers to determine whether the required level of security has been achieved. The major concern is to assessif the system provides the necessary security measures to protect against intrusions. When conducting an evaluation, ethical hackers aim to answer three fundamental questions:

1. What can an intruder see on the target systems? Ethical hackers analyze the system to identify any potential vulnerabilities or weak- nesses that may allow unauthorized access or expose sensitive information. They examine the system from an external perspective to understand what information is accessible to potential intruders. 2. What can an intruder do with that information? Once ethical hackers have determined what information is visible, they assess the potential actions an intruder could take based on that access. This involves understanding the implications of unauthorized access, potential data breaches, or system manipulation that could occur if security measures are inadequate. By answering these questions, ethical hackers pro- vide valuable insights into the system's security posture, help- ing owners understand the vulnerabilities and potential risks. This evaluation empowers owners to make informed decisions regarding security enhancements and measures to ensure the required level of security is provided. Top of Form

Does anyone at the target notice the intruder's attempts or successes? While the first and second of these are clearly important, the third is even more important: If the owners or operators of the target systems do not notice when someone is trying to break in, the intruders can, and will, spend weeks or months trying and will usually eventually succeed. Ethical hacking is a dynamic process Ethical hacking is a dynamic process since running through the penetration test once gives the current set of security issues which subject to change over time therefore penetration testing must be continuous to ensure that system movementsand installation of new applications do not intro- duce new vulnerabilities in the system. Areas to be tested:

- Network Securities.
- Firewall and device securities.
- Application servers.
- Wireless securities.

A multi-layered assessment approach is employed to evaluate different areas of security comprehensively. Each layer focuses on specific aspects of the target system and defines how it will be assessed for vulnerabilities. It is important to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

note that protecting one layer or addressing a specific vulnerability does not guarantee overall system security. Other layers may still possess vulnerabilities that need to be identified and addressed separately. For instance, consider an application with a patched login page. While patching the login page is a step towards improving security, it does not guarantee that the entire application is secure. There may be additional vulnerabilities present in other parts of the application, such as insecure data validation, weak authorization mechanisms, or other potential weaknesses. By recognizing the need for a multi-layered approach, ethical hackers can conduct thorough assessments, targeting various areas of the system to identify vulnerabilities across different layers. This comprehensive evaluation enables owners to ad- dress vulnerabilities holistically and enhance the overall secu- rity of the system. Top of Form Companies hire ethical hackers to conduct penetration testing on their own systems inorder to identify any vulnerabilities that could be exploited by ma- licious hackers. The purpose is to strengthen the company's security measures and address any weaknesses thatcould po- tentially lead to damage. Ethical hackers utilize their skills to create a secure and foolproof environment for both the company and its clients in the online world. any actual attacks occur. By doing so, they are able to identify and address any weak links or vulnerabilities, thereby enhancing the overall security pos- ture of the company.

IV. VARIOUS ATTACKS AND TOOLS

Automatic tools have changed the world of penetration test- ing/ethical hacking, IT security researcher has been developed and currently developing different tools to make the test fast, reliable and easier task. Without automatic tools, the hacking process is slow and time consuming. **Nmap/Zen map:** Nmap is a widely used tool in the field of ethical hacking, particularly for port scanning in the second phase of the process. Originally developed for Unix/Linux systems, Nmap now also has a user- friendly Windows version available. It is highly effective for gathering information about specific websites or IP addresses. Additionally, Nmap can be used for operating system finger- printing, which helps identify the operating system running on a target system. TOR Browser, short for" Total onion route," is a free and open-source software that enables anonymous communication. It allows users to browse the Internet, chat, and send instant messages anonymously. TOR is used by a variety of individuals for bothlegitimate and illicit purposes. While TOR provides a certain level of anonymity, it is not designed to completely eradicate traces of online activity. Its purpose is to reduce the ability of websites to trace actions and data back to the user. However, itshould be noted that TOR is also utilized for illegal activities. MetaSploit is a powerful tool commonly used by attackers and penetration testers alike. Exploits, such as buffer overflow, code injection, and web application exploits, target specific vulnerabilities within systems or applications to gain unauthorized access. MetaSploit contains a comprehensive database of available exploits and is known for its ease of use. It is widely regarded as one of the best tools for penetration testing. The MetaSploit framework, a sub-project of MetaSploit, is specifically used to execute exploit code againsta machine and achieve desired objectives.

NETSTUMBLER:

NetStumbler, also known as Network Stumbler, is a Windows-based tool specifically designed for detecting and an- alyzing Wi-Fi networks. It serves a variety of purposes andis commonly used for:

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in a WLAN
- Detecting causes of wireless interference
- Detecting unauthorized access points

NetStumbler can be used for aiming directional antennas in long-haul WLAN (Wireless Local Area Network) links. By analyzing signal strength and quality, NetStumbler helps optimize the positioning and alignment of directional antennas to establish stable and reliable wireless connections over longer distances [2].

Regarding the call spoofing attack, it is a type of scam where hackers deceive individuals by impersonating a legitimate business, a neighbor, or another innocent party to obtain personal information. In a call spoofing attack, the attacker can

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

manipulate the caller ID to display any phone number oftheir choice when making calls. This attack primarily relies on Voice over Internet Protocol (VoIP) technology.

One tool commonly used for call spoofing attacks is Zoiper, a softphone software. By layering proper IP protection measures, attackers can make it difficult to trace their activities. The attacker can create A-Z SIP (Session Initiation Protocol) termination services using various websites, which can be acquired through purchase or limited- time usage. One such website mentioned iswww.compeak.com [11]. Once the SIP is created for a specific phone number, Zoiper is utilized to initiate the call and carry out the attack.

It is important to note that call spoofing attacks are illegal and unethical. They can lead to identity theft, fraud, and other mali- cious activities. Such attacks exploit vulnerabilities in commu- nication systems, and it is crucial to implement security mea- sures and awareness to prevent falling victim tothem.

• Top of Form

EMAIL/TEXT BOMBER

In Internet usage, an email/SMS bomb refers to a type of net abuse where an individual or group sends an excessive amount of email or SMS messages to overwhelm the recipient's mail- box or message box. The intention is to floodthe target with a high volume of messages, causing inconvenience, disruption, or potentially rendering the mailbox unusable. Email/SMS bombs can be executed through three main methods:

Mass Mailing: This method involves sending a massive num- ber of emails to a specific email address, often using automated tools or scripts. The goal is to overwhelm therecipient's mail- box with an influx of messages, leading to resource exhaustion and difficulty in managing legitimate emails.

List Linking: List linking is a technique where the attacker subscribes the target's email address to multiple mailing lists or newsletters without their consent. This results in an influx of unwanted emails, flooding the target's inbox and overwhelming their ability to process legitimate messages.

Zip Bombing: Zip bombing, also known as a compressed file bomb, involves creating a highly compressed file that, when extracted, expands to an enormous size. The attacker may send this file to the target's email address or attach it to an email. When the victim attempts to extract or open the file, it expands to consume an excessive amount of disk space, potentially causing system or email client crashes.

It is important to note that email/SMS bombing is considered a form of harassment, net abuse, and violation of acceptable usepolicies. It is illegal and unethical to engage in such activities, as they can cause significant disruption, inconvenience, and potential damage to individuals or organizations. Measures should be taken to protect against and mitigate the impact of such attacks, including implementing email filtering, firewalls, and user education on email security best practices.

BRUTE FORCE ATTACK:

A brute force attack is a type of cyber-attack used to un- cover user credentials or passwords by systematically trying numerous possible combinations until the correct one is dis- covered. This method involves automated tools or scripts that repeatedly generate and input different combinations of user- names and passwords to gain unauthorized access to a target system or account. • Guessing the credentials • Trial and error

Username list and Password list Tools used: Medusa,

John the reaper (Kali Linux), Metasploit, Air-crack NG. Toexecute this attack, it is done in sequential manner Brute Forcetool is used to find the username and password, once you havethe id password it must be authenticated whether the creden-tials are True or False. To get the list for username and pass-word list a tool name hydra is used in the Terminal of kali Linux. You need to know the webapp is a get or post method. The command used is: hydra -l filename.txt –p filename.txt ipaddress http –get/post Brute-force attacks can be made less ef-fective by obfuscating the data to be encoded making it more difficult for an attacker to recognize when the code has been cracked or by making the attacker do more work to test eachguess. One of the measures of the strength of an encryptionsystem is how long it would theoretically take an attacker tomount a successful brute-force attack against it. This attackcan also be done by using mobile phone application to be usedis Termux here the password and username list is required to complete the attack successfully

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

PENTESTING:

Ethical hackers employ various approaches when conducting their assessments. Two common approaches are:

Remote Network Testing: This type of test simulates an at- tack from the internet, attempting to exploit vulnerabilities in the target's network infrastructure and systems. The purpose is to identify potential security weaknesses that could be exploited by remote attackers. The test may encounter measures like border firewalls, filtering routes, or other security mechanisms designed to protect the network [7].

Social Engineering Testing: This test focuses on evaluating the human element within the target organization. It assesses whether the organization's staff members can be manipulated into divulging sensitive information to unauthorized individuals. Social engineering techniques involve attempting to de- ceive or trick employees into providing access credentials, sharing confidential information, or performing actions that com- promise security. For instance, an ethical hacker might impersonatea trusted individual or use persuasion tactics to extract information from employees. An example could be an intruder posing as a legitimate caller and contacting the organization's computer help line, attempting to obtain external telephone numbers or other sensitive details [7]. Both remote network testing and social engineering testing are essential components of a comprehensive ethical hacking process. They help identify potential vulnerabilities not only in technical systems but also in human interactions, allowing organizations to strengthen their overall security posture.

REFERENCES

[1]. "Ethical Hacking, January 2015"https://www.researchgate.net/publication/271079090ET HICAL HACKING Tools Techniques and Approaches
[2]. "Tools"http://www.ehacking.net/2011/06/top-6-ethical- hackingtools.htmlsthash.nszGZw4 y.dpuf
[3]. MetaSploit.com
[4]. "Penetration Testing" http://www.owasp.org/index.php/WebApplicationPenetrationTesting.html
[5]. http://www.corecom.com/external/livesecurity/pentest.ht ml
[6]. http://www.networkdefense.com/papers/pentest.html
[7]. Internet Security Systems, Network and Host-based Vulnerability Assessment
[8]. http://www.infosecinstitute.com/blog/ethicalhackingcom puterforensics.html
[9]. http://searchnetworking.techtarget.com/generic/0,295582, sid7gci1083 715, 00.html
[10]. http://www.owasp.org/index.php/Testing:InformationGat hering