RESEARCH ARTICLE OPEN ACCESS

Breaking Barriers: Unveiling Ethical Hacking and Penetration Testing Tactics for Secure Systems

Dr.J.Raji [*], Dr. Kavipriya K[**], Nisha M [***], Kiran D Hosagoudar[****], Sinchana N[*****], Harsha Kumar V[******]

* (Department of Mathametics,T.John Institute of Technology, Bengaluru,
Email: raji@tjohngroup.com)
** (Department of MCA,T.John Institute of Technology, Bengaluru,
Email:kavipriya@tjohngroup.com)
*** (Department of MCA,T.John Institute of Technology, Bengaluru,
Email: nishamb07@gmail.com)
**** (Department of MCA,T.John Institute of Technology, Bengaluru,
Email: kiranhosagoudar1@gmail.com)
***** (Department of MCA,T.John Institute of Technology, Bengaluru,
Email: sinchanagowda196@gmail.com)
****** (Department of MCA,T.John Institute of Technology, Bengaluru,
Email: hn7135623@gmail.com)

************************* -

Abstract:

Ethical hacking, also known as penetration testing or white-hat hacking, is a critical component of contemporary cybersecurity, aimed to identifying vulnerabilities within computer systems, networks, or applications before malicious actors can exploit them. This paper explores the significance of ethical hacking in fortifying digital defenses by discussing the utilization of authorized professionals who employ hacking techniques to enhance security measures. Specifically, the focus is on Kali Linux Software, a comprehensive penetration testing platform renowned for its extensive toolkit catering to various security testing needs. Also, the study delves into John the Ripper, a widely-used password cracking tool within cybersecurity and ethical hacking domains. The paper also delves into cryptography, emphasizing its role in in safeguarding communication and data through encryption methods. Furthermore, the paper examines the different types of hacking, categorizing them into white hat, black hat, and grey hat hacking, and underscores the growing necessity for individuals to be cognizant of ethical hacking practices amidst the escalating number of cyber threats.

Keywords — **Penetration testing, Cryptography, Hacking Techniques, Kali Linux Software, John the Ripper, White hat, Black hat**

************************* -

I. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website. People often think of hackers as criminals, but that wasn't always the case. The term "hacker" was first used by smart students at MIT in the 1960s to describe Finding new ways to improve things like machines and systems. Back then, hacking was seen as a creative and clever skill. Hacking started even before computers were connected to the internet.

In the 1970s, when computers were rare and expensive, some hackers figured out how to make free phone calls by tinkering with telephone systems.

In the 1990s, as the internet became popular, criminal activities like fraud and hacking increased. Some famous hackers, like Robert Morris and Kevin Mitnick,[1] were even put in jail for stealing information from computer networks. There are also good hackers who use their skills to help protect companies from cyber-attacks. They take courses like SEC560, [2] which teaches them how to find vulnerabilities in networks and make the

Safer, between the United States and Israel. Fig 1explain about the Stuxnet Worm.In the world of cyber security, certifications like CISM [Certified Information Security Manager] and CISSP [Certified Information Systems Security Professional] are essential. These certifications show that professionals have the skills and knowledge to manage and secure.

II. LITERATURE REVIEW

Shravan Pargaonkar et al. [3] this paper provides an in-depth exploration of security testing methodologies and emerging trends that are pivotal in safeguarding applications against evolving cyber threats. Security testing is a multidimensional practice crucial for identifying vulnerabilities, assessing risks, and fortifying software applications against cyber threats. Emerging trends like Develops integration and continuous security testing underscored the dynamic nature of security testing, emphasizing collaboration, adaptability, and strategic mitigation strategies to bolster organizations' security readiness and protect sensitive user data.

Jean-Paul A et al. [4] The paper emphasizes the critical need for periodic and effective penetration testing and ethical hacking in IOT systems to counter the increasing security threats posed by the growing number of IoT devices. Classifying and analyzing IoT hackers based on their motives and gains in a more detailed and specific way. Analytical Study: of how to assess IoT vulnerabilities in terms of IOT related risk. Oss W. Bellaby's et al [5] literature survey on an ethical framework for hacking operations likely delves into the complex intersection of cybersecurity, ethics, and hacking practices. Bellaby may explore various ethical theories and principles, such as utilitarianism, deontology, and virtue ethics, to propose dilemmas, and existing ethical frameworks in the field of cybersecurity to develop comprehensive guidelines for ethical hacking operations. Fakhrul Safitra et al. [6] this paper emphasizes the utilization of java Library Log4j and vulnerabilities in application and devices provide opportunities for malicious hackers. It involves using domain-specific information and exploit-based analysis to predict how likely it is for an intrusion to happen in each stage of a particular. Mohamed Chahine Ghanem et al. [7] This paper addresses the challenge by proposing an Expert-System Automated Security Compliance Framework (ESASCF), which streamlines security auditing processes, enhances efficiency, and empowers experts to focus on critical tasks in security compliances expected to address scientifically the real-world problem of efficiency and effectiveness related to the current VA and PT automation. Muhammad Ahmar Hassan et al. [8] This paper delves into the evolving landscape of cybersecurity within the Internet of Things (IoT) realm, highlighting the growing exposure of internet users to IoT devices and the associated security risks. Methodology used are Reconnaissance, Vulnerability assessment or Scanning, Exploitation, Post-exploitation, post-exploitation. Paul Formosaa et al. [9] this paper delves into the methodology of penetration testing and security measures to identify vulnerabilities within systems, aiming to bolster cybersecurity defenses against potential threats. Developing a principlist framework for cybersecurity ethics involves identifying and synthesizing foundational ethical principles to guide decision-making and behavior in insights for enhancing cyber security defenses in these interconnected environments. Evaluating the effectiveness and efficiency of systems, processes, or strategies to assess their impact and identify areas for improvement.

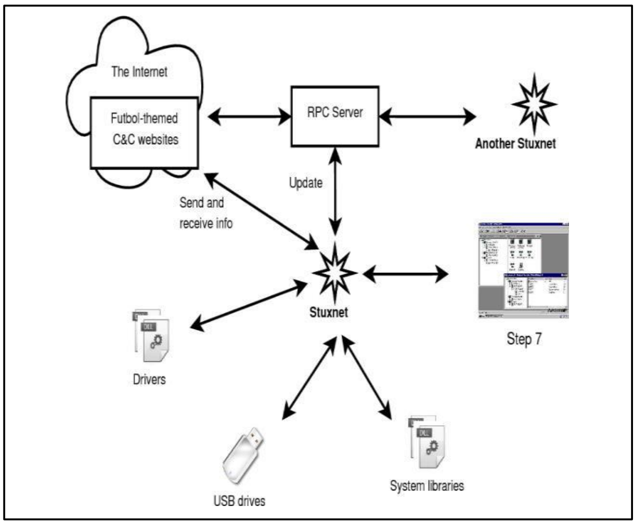

Fig . 1 The Stuxnet Worm

Cyber security is becoming increasingly recognized, the important ethical issues that cybersecurity raises are less well understood. Cyber security ethics principlist framework involves evaluating its efficacy in addressing ethical conflicts and enhancing decision-making for cybersecurity professionals. Shahid Ali et al. [10] The paper explores the effectiveness and implications of ethical hacking practices, shedding light on their role in enhancing cybersecurity measures. It approaches consists of arranging, executing, and reporting phases in which there are many stages in each process. hackers discover bugs and weaknesses and alter them according to their specification. Ethical hacking assesses its efficacy in uncovering vulnerabilities, strengthening security protocols, and mitigating cyber threats within diverse organizational contexts. Shivani Singh et al. [11] this paper delves into the methodology of penetration testing and security measures to identify vulnerabilities within systems, aiming to bolster cybersecurity defenses against potential threats. Penetration testing's role in identifying system vulnerabilities, emphasizing the need for cybersecurity measures amidst rising cyber threats. Penetration testing, when conducted effectively, helps organizations identify security vulnerabilities, mitigating major attacks and financial losses. Evaluating the effectiveness and efficiency of systems, processes, or strategies to assess their impact and identify areas for improvement. Thomas Schiller et al. [12] this study explores enhancing security awareness in smart homes and IoT networks through swarm-based cybersecurity penetration testing, aiming to fortify defenses against emerging cyber threats. Using swarm-based techniques, we conduct penetration testing to mimic real-world cyber-attacks on smart home devices and IoT networks. This involves evaluating vulnerabilities and gauging the effectiveness of security measures. Demonstrate the efficacy of swarm-based cybersecurity penetration testing in identifying vulnerabilities and improving security awareness in smart homes and IoT networks, providing valuable

Lewis Go lightly et al. [13] this study delves into the realm of ethical hacking, focusing on the performance of hacking a router and the valuable lessons learned in the process. It aims to shed light on the ethical considerations and technical challenges involved in such endeavors. conducting ethical hacking experiments targeting routers, employing a combination of penetration testing tools and techniques to identify vulnerabilities and potential attack vectors. The results highlight the efficacy of ethical hacking in uncovering vulnerabilities within router systems and the critical importance of addressing these vulnerabilities to enhance network security. it reveals the effectiveness of ethical hacking methodologies in identifying and exploiting vulnerabilities within router systems, providing valuable insights into the strengths and weaknesses of network security. Prabhat Kumar Sahu et al. [14] this review paper provides an overview of ethical hacking, examining its role, significance, and ethical considerations in cybersecurity. It aims to elucidate the methodologies, tools, and principles guiding ethical hacking practices. Comprehensive review of existing literature, scholarly articles, and case studies related to ethical hacking. importance of ethical hacking as a proactive approach to cybersecurity, emphasizing its effectiveness in identifying and mitigating vulnerabilities before they are exploited by malicious actors. Evaluates the efficacy and impact of ethical hacking. Del-Real et al. [15] the potential for ethical hacking to reduce security vulnerabilities in software systems, Cybersecurity experts in Spain recognize the importance of ethical hackers in enhancing cybersecurity governance. understand the effectiveness and feasibility of leveraging ethical hacking as a means to enhance cybersecurity in Spain. Which are only permitted when there is a contract between the company and the security analyst. Fredrik Heidinga at al. [16] the proliferation of the Internet of Things (IoT) and the connectivity it brings, the Series of penetration tests conducted on various products from connected households revealed 17 vulnerabilities. Represents the most comprehensive assessment of penetration testing on connected household products. Which are only permitted when there is a contract between the company and the security analyst. Fouz Barma et al. [17] the proactive approach of ethical hacking, which allows for the identification and mitigation of security vulnerabilities before they can be exploited by malicious actors. Methodology for conducting penetration testing, specifically focusing on the reconnaissance and enumeration phases. Methodical framework that provides a technical guide for the reconnaissance and enumeration phases of the penetration testing lifecycle. Mrittikaa das et al. [18] the role of ethical hacking in addressing the ever-growing threat of cyber-attacks. It portrays ethical hacking solely as a solution to cyber threats, potentially overlooking ethical and legal considerations. Emphasize the importance of ethical hacking in addressing cybersecurity challenges in today's technologically driven world. Contribute to enhancing cybersecurity measures and fostering a more positive perception of ethical hackers. Ivan nedyalkov et al [19] the increasing focus on the communication capabilities of power electronic devices (PEDs) in the context of their connection to IP networks and the Internet. Increased vulnerability of power electronic devices (PEDs) due to their connection to IP networks and the Internet. Evaluate the level of network security in power electronic devices. Assess the security of data exchange between power electronic devices. Syed Zain ul Hassan et al. [20] Identifying weaknesses in software systems, networks, and applications before they are exploited by malicious actors. Generate false positives, leading to wasted time and resources in investigating non-existent vulnerabilities. Exploring the integration of automation and artificial intelligence (AI) in ethical hacking tools to improve accuracy and efficiency. Conducting a study to evaluate the effectiveness of different ethical hacking tools and techniques in identifying and mitigating vulnerabilities across various stages of the SDLC. Denys Mishchenko et al. [21] Increased reliability, security, and sustainability of power systems achieved through digitalization. Highlights the persistent challenge of cyber-physical threats to digitalized power systems without providing specific examples. Digitalization of Power Systems. he integration of digital technologies such as sensors, real-time communication, IoT, and data analytics is rapidly transforming power systems. Cybersecurity testbeds are essential tools in ensuring the resilience and security of power systems against cyber-physical threats in an increasingly digitized landscape. Esra Abdulla if Altulaihan et al. [22] a survey on web application penetration testing offers insights into prevalent vulnerabilitie. Common vulnerabilities such as SQL injection and XSS are identified, along with effective penetration testing tools and techniques. Common vulnerabilities such as SQL injection and XSS are identified, along with effective penetration testing tools and techniques. Mohamed Hamza Javed et al. [23] Ethical hacking of a smart camera can uncover vulnerabilities in its security protocols, allowing manufacturers to patch, unauthorized access to a smart camera through ethical hacking could potentially lead to privacy breaches. Through ethical hacking, vulnerabilities such as weak authentication mechanisms, insecure communication protocols, or inadequate encryption methods may be discovere, Smart cameras aims to identify vulnerabilities in their security protocols, yet challenges exist in balancing the need for rigorous testing. Mujahid Tabassum, Saju Mohanan et al. [24] Ethical hacking with Kali and Metasploit allows for comprehensive testing of security measures. Through ethical hacking, weaknesses such as outdated software or weak passwords can be uncovered, enabling proactive security measures to be implemented. Understanding the effectiveness and limitations of ethical hacking and penetration testing using Kali Linux and the Metasploit Framework. Giorgia Lorenzini et al. [25] ethical hackers bolster healthcare cybersecurity by proactively identifying vulnerabilities, ensuring patient data confidentiality and system integrit, Healthcare may inadvertently disrupt critical systems or patient care if not conducted with caution and adherence to regulatory guidelines. Uncover vulnerabilities such as weak authentication methods or outdated software, enabling healthcare organizations to fortify their cybersecurity defenses. Uncover vulnerabilities such as weak authentication methods or outdated software, enabling healthcare organizations to fortify their cybersecurity defenses. Petar Lachkov ET at. [26] Vulnerability assessment and penetration testing simulate real-world attacks, helping identify and mitigate security flaws, Over-reliance on automated tools may overlook certain vulnerabilities or fail to accurately. Through simulated attacks, vulnerabilities such as injection flaws or insecure configurations are uncovered. Investigating vulnerability assessment and penetration testing methods aims to enhance application security. De Paoli et al. [27] Qualitative studies allow for a deep exploration of the experiences, perspectives, and practices of penetration testers, Qualitative studies typically involve small sample sizes and specific contexts, limiting the generalizability of findings to other organizations or settings. Qualitative studies typically involve small sample sizes and specific contexts, limiting the generalizability of findings to other organizations or settings. Revolves around conducting a qualitative study on penetration testers and exploring what their experiences and insights can reveal about information security within organizations. Mariam Alhamed et al. [28] a systematic review ensures a comprehensive understanding of the existing literature on penetration testing in network, Systematic reviews may be subject to publication bias, as they rely on published literature, potentially missing unpublished studies or industry reports. Identification of common vulnerabilities targeted and discovered during penetration testing in networks, such as misconfigurations, software flaws. Investigating the role of automation, artificial intelligence (AI), and machine learning (ML) in enhancing the effectiveness and efficiency of network penetration testing. R. Sri Devi et al. [29] Identification of security vulnerabilities in web applications, including common issues like SQL injection, cross-site scripting (XSS), and authentication flaws, Ethical hacking tests may generate false positives (reporting vulnerabilities that don't exist) or false negatives (missing actual vulnerabilities), requiring manual verification and validation. Evaluate the effectiveness of ethical hacking in identifying various types of vulnerabilities in web applications. Investigate the development and integration of automated tools and algorithms for detecting vulnerabilities in web applications. Sahil Prasad Bejo et al. [30] investigate the effectiveness of advanced key loggers in detecting and preventing cyber threats such as phishing attacks, credential theft, and unauthorized access, examine potential privacy concerns and ethical considerations related to the use of keyloggers, including data collection, storage, and access. Present empirical results from testing the advanced keylogger in various cyber threat scenarios, including simulated attacks and real-world. Identify the gaps in existing literature or practical solutions that the research aims to address.

Ashwini Kumar Dautaniya ET all [31]. In a review of ethical hacking issues, methodology involves the use of various tools and techniques to identify and mitigate security vulnerabilities. Results are typically measured by the number and severity of vulnerabilities discovered, as well as the effectiveness of implemented countermeasures.

Performance analysis evaluates the overall efficacy of the ethical hacking process, including its ability to enhance system security, protect sensitive data, and mitigate risks of unauthorized access or data breaches. Anand Kumar Mishra et al.[32] In a systematic review on network security issues and threats, methodology encompasses the examination of various security measures such as firewalls, encryption protocols, intrusion detection systems, and access control mechanisms. Performance analysis involves assessing the effectiveness of these measures in preventing unauthorized access, data breaches, and network disruptions. Results are typically evaluated based on the identification of common threats, vulnerabilities, and emerging attack vectors, as well as the development of strategies to mitigate these risks and enhance overall network security posture. Maryam Roshanaei et al. [33] This books explains about the where mobile devices have become an integral part of our daily lives, ensuring the security of mobile applications has become increasingly crucial. Mobile penetration testing, a specialized subfield within the realm of cybersecurity, plays a vital role in safeguarding mobile ecosystems against the ever-evolving landscape of threats. The ubiquity of mobile devices has made them a prime target for cybercriminals, and the data and functionality accessed through mobile applications make them valuable assets to protect. Mobile penetration testing is designed to identify vulnerabilities, weaknesses, and potential exploits within mobile applications and the devices themselves.

III. ABOUT HACKING

Hacking in cyber security refers to the misuse of devices like computers, smartphones, tablets, networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity. A traditional view of hackers is a lone rogue programmer who is highly skilled in coding and modifying computer software and hardware systems. But this narrow view does not cover the true technical nature of hacking. Hackers are increasingly growing in sophistication, using stealthy attack methods designed to go completely unnoticed by cybersecurity software and IT teams. They are also highly skilled in creating attack vectors that trick users into opening malicious attachments or links and freely giving up their sensitive personal data. As a result, modern-day hacking involves far more than just an angry kid in their bedroom. It is a multibillion-dollar industry with extremely sophisticated and successful techniques. Popularly, hackers are referred to someone who penetrates into computer network security systems. It is the hackers who built Internet and make www to work. The operating system UNIX is a gift from hackers too. Originally, the term hacking was defined as-“ A person who enjoys learning the details of computer systems and how to stretch their capabilities-as opposed to most users of computers, who prefer to learn only the minimum amount necessary. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming. Unlike malicious hackers, ethical hackers have the permission and approval of the organization which they’re hacking into. Learn how you can build a career from testing the security of the network to fight cybercrime and enhance information security. Ethical Hacking as a practice includes assessing and finding the cracks in a digital system that a malicious hacker can take advantage of. These cracks assist the malicious hacker in providing an effortless way to enter and harm the system or reputation of the hacking victim. Thus, a certified ethical hacker will solidify the present security levels while finding any loopholes that may be exploited. Hacking professionals must keep ethics in mind and provide desired cyber security to individuals, firms, or governments from the threat of malicious hacking and security breaches. Besides, ethical Hacking is done with the consent of the concerned clients to enhance the safety of their online presence.CEH training online is a wonderful way to understand and implement the key concepts of ethical hacking and ways to do it right. These training programs help you learn a wide range of skills and methods to employ them and safeguard sensitive information on the internet. online presence.CEH training online is a wonderful way to understand and implement the key concepts of ethical hacking and ways to do it right. These training programs help you learn a wide range of skills and methods to employ them and safeguard sensitive information on the internet.

IV. TYPES OF HACKING

Here are three types of Hackers – White Hat, Black Hat, and Gray Hat Hackers. White Hat Hackers – These are the "Ethical Hackers" who attempt to hack into a system for the benefit and security of the system. This type of hacking is legal and is used by individuals, big and small firms, and even the government to test their systems, find any weakness and fix it. White Hat hackers work with the mentality of the malicious hackers but with good intention. They employ different methods to breach the security walls via vulnerability assessments, penetration testing, etc. The system owners often employ these hackers. Black Hat Hackers – As the name suggests, these types of hackers try to gain unauthorized access to security systems and data systems with the intent to cause harm. Their objective can be stealing sensitive information (which they can sell illegally), halt the operations process of a firm, damage the system permanently, etc. All of this is an illegal and punishable offense. Gray Hat Hackers – These types of hackers are somewhere in the middle of the White Hat and the Black Hat hackers. That is because these hackers exploit the weaknesses of a system without the owner's permission, but it is not done with any malicious intent. These hackers do this for their fun or to learn to hack, but once they are successful, they usually inform the owner about the weak point. Even though this type of hacking is done without malicious intent, it is indeed an offense. Therefore, if someone is interested in learning ethical hacking, the best course of action is to enroll in an introduction to an ethical hacking course in Hindi or English. Here Fig 2 Explains about the type of hackers

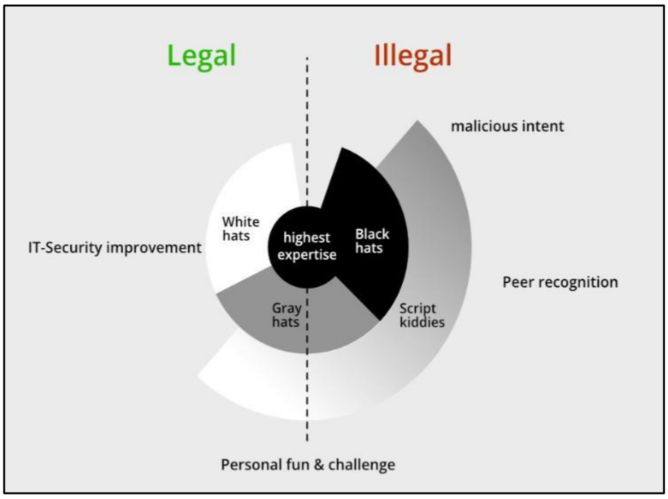

Fig.2 TYPES OF HACKING/HACKER

V. STEPS IN PEN TESTING

Pen testing providers may have varying approaches to their tests. In general, the following six activities are involved in conducting a pen test: First step is Prepare for the test, Use this phase to gather relevant information, secure approval from management and outline steps for the test.Next Construct a plan, Determine the tools needed to examine the state of the testing candidate. This includes evaluating how security is implemented and where vulnerabilities or alternate access methods may exist.Build a team, Gather the appropriate pen testers to conduct the test.

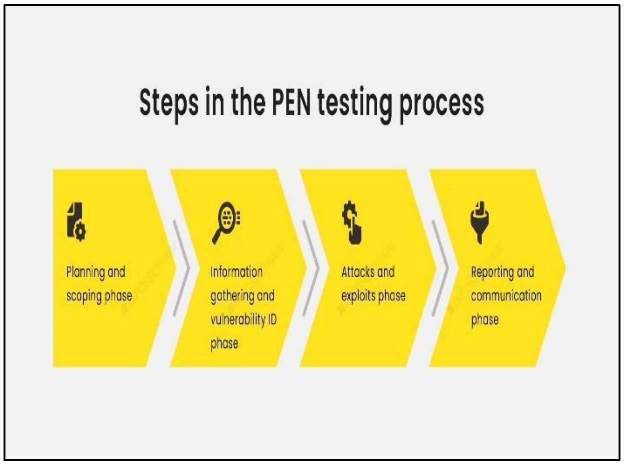
Steps in the PEN testing process
Planning and scoping phase
Information gathering and vulnerability ID phase
Attacks and exploits phase
Reporting and communication phase

Fig. 3 STEPS IN PEN TESTING

In-house and third-party experts may be needed.Find the target, Decide what data and systems are being targeted.Perform penetration, Use a variety of techniques to bypass the target system's existing security measures, such as firewalls and intrusion detection systems. Establish a foothold position over designated systems and resources, all while trying to remain undetected. Extract data and other evidence for reports.Conduct data analysis and reporting, Examine and analyze the data collected during the pen test, and identify remediation steps. Summarize the results of the tests, including what vulnerabilities were detected and exploited and how to fix them, in a report for company management.Here Fig 3 Explains Steps in pen testing.

VI. TOOLS USED IN ETHICAL HACKING

A. JOHN THE RIPPER

Currently available for many versions of UNIX(11 are officially supported, not counting different architectures),DOS,Win32,BeOS and Open VMS,John the ripper is a fast password cracker.Its primary purpose is to detect weak UNIX passwords.It supports several crypt(3)password hash types,which are most commonly found on various UNIX versions, as well as Kerberos AFS, and Windows NT/2000/XP LM hashes.John the ripper has its own optimized modules for use.

1)MODES: *John the Ripper supports several modes for cracking passwords:Wordlist mode - The simplest mode, this compares passwords against a list of words in a text file.Single-crack mode – Faster than wordlist mode, this uses logon or GECOS information for cracking passwords. It limits the cracking process to the accounts related to the logon information. If more than one user has the same password, it repeats the comparison of guessed passwords.Incremental mode – The most powerful mode used by John the Ripper, this attempts all possible combinations of letters, numbers, and special characters. It is used for conducting brute-force attacks.External mode – External mode is defined by using the [List.External: Mode] section of the john.ini file. Here, "mode" is the name of the external mode.External mode can be used to specify customized functions for trying passwords; these customized functions are added to the [List.External: Mode] section.*

B. CRYPTOGRAPHY

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce. Modern cryptography techniques include algorithms and ciphers that enable the encryption and decryption of information, such as 128-bit and 256-bit encryption keys. Modern ciphers, such as the Advanced Encryption Standard (AES), are considered virtually unbreakable.A common cryptography definition is the practice of coding information to ensure only the person that a message was written for can read and process the information. This cybersecurity practice, also known as cryptology, combines various disciplines like computer science, engineering, and mathematics to create complex codes that hide the true meaning of a message.Cryptography can be traced all the way back to ancient Egyptian hieroglyphics but remains vital to securing communication and information in transit and preventing it from being read by untrusted parties. It uses algorithms and mathematical concepts to transform messages into difficult-to-decipher code through techniques like cryptographic keys and digital signing to protect data privacy, credit card transactions, email, and web browsing.There are many types of cryptographic algorithms available. They vary in complexity and security, depending on the type of communication and the sensitivity of the information being shared.Here Fig 4 explains the Steps of Cryptography.

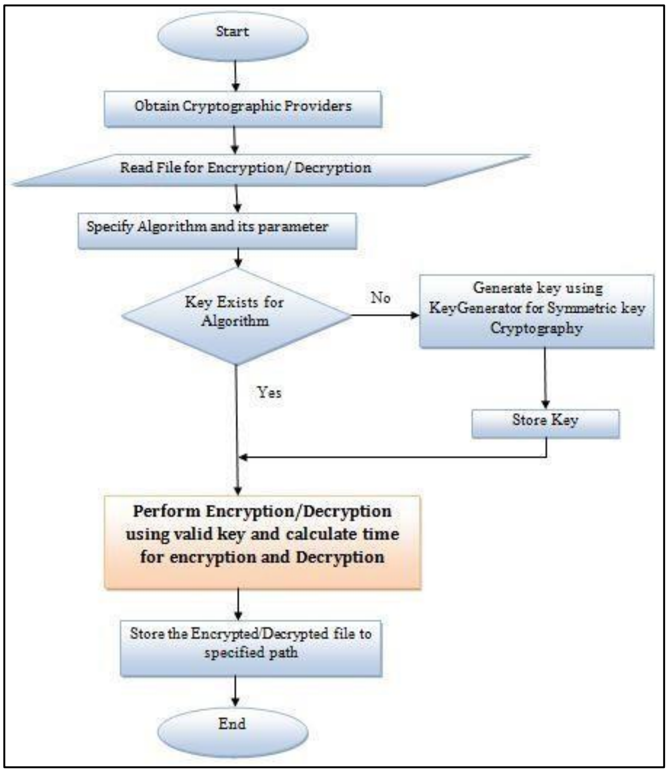
Start
Obtain Cryptographic Providers
Read File for Encryption/ Decryption
Specify Algorithm and its parameter
Key Exists for Algorithm
No
Generate key using KeyGenerator for Symmetric key Cryptography
Yes
Store Key
Perform Encryption/Decryption using valid key and calculate time for encryption and Decryption
Store the Encrypted/Decrypted file to specified path
End

Fig .4 Steps of Cryptography

C. SPOOFING

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad actor gains access in order to execute a larger cyber attack such as an advanced persistent threat or a man-in-the-middle attack.Successful attacks on organizations can lead to infected computer systems and networks, data breaches, and/or loss of revenue—all liable to affect the organization's public reputation. In addition, spoofing that leads to the rerouting of internet traffic can overwhelm networks or lead customers/clients to malicious sites aimed at stealing information or distributing malware.

Tools using spooking are Mausezahn is a fast network traffic generator written in C which allows the user to craft nearly every possible and "impossible" packet. Since version 0.31 Mausezahn is open source in terms of the GPLv2. Herbert Haas, the original developer of Mausezahn, died on 25 June 2011. The project has been incorporated into the netsniff-ng toolkit, and continues to be developed there.Second one isArpspoof the purpose of arpspoofing is often related to network security testing or malicious activities. For security testing, it can be used to detect vulnerabilities in a network's.

VII. KALI LINUX

Kali Linux is a Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security. The software is based on the Debian Testing branch: most packages Kali uses are imported from the Debian repositories. Kali Linux has approximately 600 penetration-testing programs (tools), including Armitage (a graphical cyber attack management tool), Nmap (aportscanner), Wireshark (a packetanalyzer), metasploit (penetration testingframework), JohntheRipper (a password cracker), sqlmap (automatic SQL injection and database takeover tool), Aircrack-ng (a softwaresuite for penetration-testing wireless LANs), Burp suite and OWASP ZAP web application security scanners, etc. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous information security testing Linux distribution based on Knoppix. The tagline of Kali Linux and BackTrack is "The quieter you become, the more you are able to hear", which is displayed on some backgrounds, see this example.Kali Linux's popularity grew when it was featured in multiple episodes of the TV series Mr. Robot. Tools highlighted in the show and provided by KaliLinuxincludeBluesniff, Bluetooth Scanner (btscanner), John the Ripper, Metasploit Framework, Nmap, Shellshock, and Wget. Kali Linux has a dedicated project set aside for compatibility and porting to specific Android devices, called Kali NetHunter. It is the first open source Android penetration testing platform for Nexus devices, created as a joint effort between the Kali community member "BinkyBear" and Offensive Security. It supports Wireless 802.11 frame injection, one-click MANA ARP protocol implementation. However, it can also be used maliciously, such as in man-in-the-middle attacks, where an attacker intercepts communication between two parties by spoofing ARP messages to make devices believe they are communicating directly with each other when, in reality, the attacker is intercepting and possibly altering the traffic.And Ettercap is a comprehensive suite for man-in-the-middle attacks on LAN (Local Area Network). It allows users to intercept, sniff, and manipulate data packets in a network. Ettercap is designed for both security professionals conducting penetration testing and network .

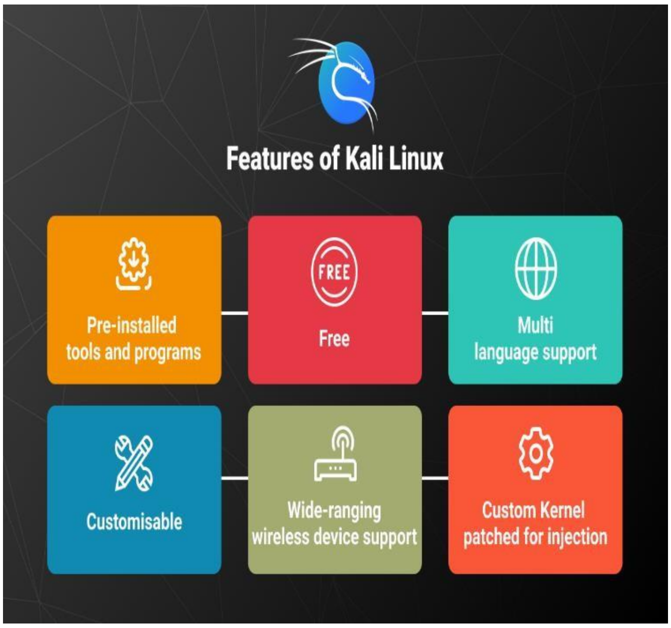
Features of Kali Linux
Pre-installed tools and programs
FREE
Free
Multi language support
Customisable
Wide-ranging wireless device support
Custom Kernel patched for injection

Fig. 5 KALI LINUX

Evil Access Point setups, HID keyboard (Teensy like attacks), as well as Bad USB MITM attacks. BackTrack (Kali's predecessor) contained a mode known as forensic mode, which was carried over to Kali via live boot. This mode is very popular for many reasons, partly because many Kali users already have a bootable Kali USB drive or CD, this option makes it easy to apply Kali to a forensic job. When booted in forensic mode, the system doesn't touch the internal hard drive or swap space and auto mounting is disabled. However, the developers recommend that users test these features extensively before using Kali for real world forensics.Here Fig 5 explains the features of Kali Linux

VIII. CONCLUSION

In conclusion, ethical hacking is a crucial discipline in the field of cybersecurity. By leveraging ethical hacking methodologies individuals and organizations can identify and address vulnerabilities, strengthen their defenses, and protect sensitive information from malicious threats. A proactive approach and a commitment to continuous learning, ethical hackers contribute significantly to the resilience of our digital world. Remember, ethical hacking is not about exploiting vulnerabilities for personal gain but about fortifying our digital infrastructure to ensure a safer and more secure cyberspace. Ethical hacking is not about causing harm but rather about preventing it. It promotes a culture of security awareness, continuous improvement, and proactive defense against evolving cyber threats. By embracing ethical hacking practices, individuals and organizations can stay one step ahead in the ongoing battle against cybercrime.

REFERENCES

[1] https://www.knowledgehut.com/blog/security/history-of-ethical-hackers-May.2024- Learn the latest digital skills for tomorrow's jobs

[2] https://www.sans.org/brochure/course/network-penetration-testing-ethical-hacking/3425-May.2024India's most trusted source for cyber security training, certification, and research.

[3] S. Pargaonkar, "Advancements in Security Testing: A Comprehensive Review of Methodologies and Emerging Trends in Software Quality Engineering," International Journal of Science and Research (IJSR), vol. 12, no. 9, pp. 61–66, Sep. 2023, doi: 10.21275/sr23829090815.

[4] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 280–308, Jan. 2023, doi: 10.1016/j.iotcps.2023.04.002.

[5] R. W. Bellaby, "An Ethical Framework for Hacking Operations," Ethical Theory and Moral Practice, vol. 24, no. 1, pp. 231–255, Mar. 2021, doi: 10.1007/s10677-021-10166-8.

[6] F. Maulana, H. Fajri, M. F. Safitra, and M. Lubis, "Unmasking log4j's Vulnerability: Protecting Systems against Exploitation through Ethical Hacking and Cyberlaw Perspectives," in Proceedings of the 9th International Conference on Computer and Communication Engineering, ICCCE 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 311–316. doi: 10.1109/ICCCE58854.2023.10246082.

[7] M. C. Ghanem, T. M. Chen, M. A. Ferrag, and M. E. Kettouche, "ESASCF: Expertise Extraction, Generalization and Reply Framework for Optimized Automation of Network Security Compliance," IEEE Access, vol. 11, pp. 129840–129853, 2023, doi: 10.1109/ACCESS.2023.3332834.

[8] M. A. Hassan, "'Demonstration of cyber security through Penetration testing on IP camera.'" [Online]. Available: https://www.researchgate.net/publication/368608725

[9] P. Formosa, M. Wilson, and D. Richards, "A principlist framework for cybersecurity ethics," Comput Secur, vol. 109, Oct. 2021, doi: 10.1016/j.cose.2021.102382.

10] S. Rafiq, S. Zain Ul Hassan, M. Waseem Iqbal, S. Ali, S. U. Zain Hassan, and A. Arshad, "An empirical analysis of ethical hacking," 2023, doi: 10.17605/OSF.IO/2UBJ4.

[11] G. Srivastava, S. Singh, S. Singh, and S. Kumar, "Penetration Testing And Security Measures To Identify Vulnerability Inside The System," vol. 25, no. 3, pp. 50–64, doi: 10.9790/0661-2503015064.

[12] T. Schiller, B. Caulkins, A. S. Wu, and S. Mondesire, "Security Awareness in Smart Homes and Internet of Things Networks through Swarm-Based Cybersecurity Penetration Testing," Information (Switzerland), vol. 14, no. 10, Oct. 2023, doi: 10.3390/info14100536.

[13] L. Golightly, V. Chang, and Q. A. Xu, "Towards Ethical Hacking-The Performance of Hacking a Router and Lessons Learned."

[14] K. Sahu and B. Acharya, "A REVIEW PAPER ON ETHICAL HACKING," International Journal of Advanced Research in Engineering and TTechnology (IJARET), vol. 11, no. 12, pp. 163–168, 2020, doi: 10.34218/IJARET.11.12.2020.018.

[15] C. Del-Real and M. J. Rodriguez Mesa, "From black to white: the regulation of ethical hacking in Spain," Information and Communications TTechnology Law, vol. 32, no. 2, pp. 207–239, 2023, doi: 10.1080/13600834.2022.2132595.

[16] F. Heiding, E. Süren, J. Olegård, and R. Lagerström, "Penetration testing of connected households," Comput Secur, vol. 126, Mar. 2023, doi: 10.1016/j.cose.2022.103067.

[17] F. Barman, N. Alkaabi, H. Almenhali, M. Alshedi, and R. Ikuesan, "A Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle." [Online]. Available: https://www.kali.org/get-kali/#kali-virtual-machines

[18] Mrittikaa Das, "ETHICAL HACKING-HOW IT OPERATES," Cyber Law Reporter , vol. 2, no. 2, pp. 19–31, 2023.

[19] I. Nedyalkov, "Study the Level of Network Security and Penetration Tests on Power Electronic Device," Computers, vol. 13, no. 3, Mar. 2024, doi: 10.3390/computers13030081.

[20] S. Z. A. Syed Zain ul Hassan, "The Importance of Ethical Hacking Tools and Techniques in Software Development Life Cycle," International Journal of Advanced Trends in Computer Science and Engineering, vol. 10, no. 3, pp. 2042–2049, Jun. 2021, doi: 10.30534/ijatcse/2021/791032021

[21] D. Mishchenko, I. Oleinikova, L. Erdodi, and B. R. Pokhrel, "Multidomain Cyber-Physical Testbed for Power System Vulnerability Assessment," IEEE Access, vol. 12, pp. 38135–38149, 2024, doi: 10.1109/ACCESS.2024.3375401.

[22] E. A. Altulaihan, A. Alismail, and M. Frikha, "A Survey on Web Application Penetration Testing," Electronics (Switzerland), vol. 12, no. 5. MDPI, Mar. 01, 2023. doi: 10.3390/electronics12051229.

[23] Mohammed Hamza Javed, "Internet of Things Hacking: Ethical Hacking of a Smart Camera," 2023.

[24] T. S. Mujahid Tabassum, "[22]Mujahid Tabassum," International Journal of Innovation in Computational Science and Engineering , vol. 2, no. 1, pp. 9–22, 2021.

[25] G. Lorenzini, D. M. Shaw, and B. S. Elger, "It takes a pirate to know one: ethical hackers for healthcare cybersecurity," BMC Med Ethics, vol. 23, no. 1, Dec. 2022, doi: 10.1186/s12910-022-00872-y.

[26] P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing," Journal of Web Engineering, vol. 21, no. 7, pp. 2187–2208, 2022, doi: 10.13052/jwe1540-9589.2178.

[27] S. De Paoli and J. Johnstone, "A qualitative study of penetration testers and

what they can tell us about information security in organisations," Information TTechnology and People, 2023, doi: 10.1108/ITP-11-2021-0864.

[28] M. Alhamed and M. M. H. Rahman, "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions," Applied Sciences (Switzerland), vol. 13, no. 12. MDPI, Jun. 01, 2023. doi: 10.3390/app13126986.

[29] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," in Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020, Institute of Electrical and Electronics Engineers Inc., Jun. 2020, pp. 354–361. doi: 10.1109/ICOEI48184.2020.9143018.

[30] S. P. Bejo, B. Kumar, P. Banerjee, P. Jha, A. N. Singh, and M. K. Dehury, "Design, Analysis and Implementation of an Advanced Keylogger to Defend Cyber Threats," in 2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 2269–2274. doi: 10.1109/ICACCS57279.2023.10112977.

[31] A. Kumar Dautaniya and A. Jha, "ETHICAL HACKING ISSUES: A REVIEW," INDIAN JOURNAL OF TECHNICAL EDUCATION, vol. 8, no. 2, pp. 1–14, 2020.

[32] A. K. Mishra, "EasyChair Preprint A Systematic Review on Network Security Issues and Threats A Systematic Review on Network Security Issues and Threats," 2024.

[33] M. Roshanaei, "Enhancing Mobile Security through Comprehensive Penetration Testing," Journal of Information Security, vol. 15, no. 02, pp. 63–86, 2024, doi: 10.4236/jis.2024.152006.