The Importance of Ethical Hacking Tools and Techniques in Software Development Life Cycle

Syed Zain ul Hassan, Saleem Zubair Ahmad
msse-f20-010@superior.edu.pk
Superior University, Lahore, Punjab, Pakistan

Abstract
Ethical hackers are using different tools and techniques to encounter malicious cyber-attacks generated by bad hackers. During the software development process, development teams typically bypass or ignore the security parameters of the software. Whereas, with the advent of online web-based software, security is an essential part of the software development process for implementing secure software. Security features cannot be added as additional at the end of the software deployment process, but they need to be paid attention throughout the SDLC. In that view, this paper presents a new, Ethical Hacking - Software Development Life Cycle (EH-SDLC) introducing ethical hacking processes and phases to be followed during the SDLC. Adopting these techniques in SDLC ensures that consumers find the end-product safe, secure and stable. Having a team of penetration testers as part of the SDLC process will help you avoid incurring unnecessary costs that come up after the data breach. This research work aims to discuss different operating systems and tools in order to facilitate the secure execution of the penetration tests during SDLC. Thus, it helps to improve the confidentiality, integrity, and availability of the software products.

Keywords
Ethical Hacking, Software Security, Software Quality Assurance, Software Testing, Ethical Hacking SDLC, Secure SDLC, Penetration testing.

1. INTRODUCTION

During the software development process, a minor flaw in software can result in a loss of millions or even billions of dollars [1]. On a larger scale, enterprise software is not immune to these vulnerabilities. Among the most popular, malicious attacks can seriously damage a company's business and credibility. As information security becomes more vulnerable in the hands of malicious attackers over time, having a ubiquitous presence on the internet becomes increasingly important. So, countermeasures must be taken immediately to strengthen security. The application host is one of the common routes that malicious hackers search for to gain access to the network.

Manuscript received June 5, 2023
Manuscript revised June 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.6.21

1.1 Ethical Hacking.

Ethical hackers study and practice hacking in a competent way, to improve the security of the system [2] by legally breaking into software and digital devices to find vulnerabilities.

1.2 Phases of Ethical Hacking.

To break a network or device, ethical hackers use the same five-step hacking technique [2]. The ethical hacking process starts with searching for different ways to break into a system, leveraging bugs, maintaining consistent access to the system,
and finally clearing one's tracks. The following figure 1 shows the phases followed by Ethical Hacker [3]:

Fig. 1. Phases follow by the ethical hacker [3].

1.3 Penetration testing [4].

A penetration or pen test is a structured attempt to break into a device or network in order to find security flaws. Pentest uses the same tactics that a hacker would use in a normal attack. This option enables sufficient steps to be taken to remove vulnerabilities before they can be exploited by unauthorized people. The different types of penetration tests include:

- **Network Penetration testing [5].**

Network penetration testing is a legal and secure way to find security holes in an organization's network's architecture, implementation, or service. The testers analyze and hack the test target to see whether modems, remote access devices, and maintenance connections can be used to penetrate it.

- **Application security testing [5].**

Application security testing is the method of finding security flaws and bugs in source code in order to make them more robust to security threats.

- **Physical Penetration Testing [6].**

A physical penetration test's main advantage is that it exposes bugs and defects in physical controls (locks, barriers, cameras, or sensors) so that they can be fixed quickly.

1.4 Use of Ethical Hacking in SDLC model.

The technical implication is that the software is first engineered and then later tested for vulnerabilities, a security review is performed at the end. The security patching of the developed software is typically used to patch the vulnerabilities, although this is far more expensive than fixing the root cause. If the bugs and data breaches are resolved after the deployment phase of SDLC, by using penetration testing, the software at the end, will cost much less than the previous calculation [7]. As the threat environment has shifted, companies are focused on creating safer applications that will allow them to increase their profit and consumer appeal.

After the deployment phase of SDLC, the use of a team of penetration testers helps to avoid the costs that would otherwise arise from a data breach, ethical hacking techniques help in the following ways:

- To find vulnerabilities and patch them timely.
- To find any data breach that could have already occurred after deployment.
- Other flaws, such as hardware and software loopholes, may be discovered during penetration testing to assist in determining other flaws.
- To aid in the process of continuous defense.
- Internal penetration evaluations can help decide whether policies and procedures are existing, well understood, and enforced.
- Scheduled penetration testing, lowers long-term costs and losses by remedying the number of vulnerabilities right away.

Penetration testing reports provide the management with detailed documentation of where the company stands in terms of its information protection. Recorded reports often serve as a rationale for the costs associated with acquiring the associated technologies to strengthen the protection.

1.5 Objectives of Ethical hacking during SDLC:

- Preventing unauthorized access to the data and illegal attempts by hackers [8] by using penetration testing during software development.
- Performs vulnerability scan during development.
- Fixed the bugs and security loopholes [8] during software development.
- Protection of data by using encryption techniques [8].
-

2. LITRATURE REVIEW

Several recent ethical hacking research papers only discussed the techniques, tools used by hackers after they gained access to the system. However, the focus of our research paper will be on how to incorporate Ethical Hacking techniques into the SDLC model in order to avoid the costs that would otherwise result from the data breach of newly developed software.

In this paper, Sonali Patil et al. describe the term hacker who is either good or bad. To gain illegal access to systems, bad hackers such as black hat, hacktivists, state-sponsored, suicide, and script kiddies are used [3]. Good hackers like white hats, often called ethical hackers, are good people who protect any organization in order to keep their information in a secured manner from bad hackers. The different types of activities performed by ethical hackers to evaluate the system’s security. Sonali Patil et al. describe the five different phases adopted by pen

tester/ethical hackers to preserve the protection of devices on the network, which includes reconnaissance of data, scanning of a network, enumeration of data, gaining access to the network, maintaining access to the network (don't lose the connection), and clearing/removing logs and tracks [3]. The author explains different sets of tools for the reconnaissance phases, which are: Who is Lookup, Google search engine, NS Lookup. Nmap Ping, Tracert, Zenmap, Netcraft, and Nikto Website Vulnerability are tools for the scanning phase.Fluxion, Wireshark, pwdump7, and other tools can be used to gain access to the phase.For Maintaining the access phase tools include Metasploit Pen Testing Software etc. For clearing tracks, phase tools include Metasploit Pen Testing Software, OSForensic. The authors explain that these tools are platform-dependent and run on various types of operating systems, including Linux, Windows macOS, Fedora, DOS, Open VMS, Unix, Solaris, BSD, Microsoft Windows, AIX, HP-UX, SunOS, WindowsNT, IRIX, Sun OS, Ubuntu. Moreover, the authors describe these kinds of methods for hacking which are based on social engineering are called phishing attacks [3]. Through phishing attack techniques, an attacker tries to acquire sensitive information by sending the link to the device. By clicking on this bogus link and entering credentials, the user directly reaches the attacker's machine's Internet Protocol (IP) address, and the hacker phishes the user. The authors conclude that to protect and secure data/information from hackers, there is a need for ethical hacking techniques in the cybersecurity field [3].

In this paper, Nimesha Nishadhi explained ethical hacking as a technique that is used to increase online security [9]. He investigates ethical hacking, its types, ethics, methodology, and tools used in the ethical hacking process as it relates to cybersecurity [9].The author proposed a solution for the ethical hacker security life cycle, which begins with planning to find vulnerabilities in a specific system, policy implementation of the ethical process, monitoring and managing the threat, intrusion detection of the system through the ethical life cycle, security assessment of vulnerable systems, risk involved during analysis, and detailed analysis of t.The author describes a method for collecting vulnerabilities for ethical hacking, a system that includes the level of security, exploit range, recognizing the network, re-correcting network vulnerability, securing the network, capturing the information, gathering information about viruses and threats, recovering penetrating files and clearing logs, finding the weakness and alerting IT/network administrators. Furthermore, the author explains the ethical hacker's approach, beginning with the remote network: in this process, the ethical hacker discovers basic information about hardware and network devices such as IP addresses, etc. [9].

In this paper, Junyan Shi and Juanjuan Li in his article explained that the security of computer networks has become an important issue in the development phase of any computer network [10]. We must move away from security threats using advanced network security technologies and security detection software to effectively and efficiently monitor potential threats found on the network. It should raise awareness of the network security elements, improvement of morality in the whole society with the help of awareness, reduction of network interruptions, and efforts to create a secure network environment to encounter network vulnerabilities [10]. The authors described the policy to secure networks by setting a firewall on network technologies: A firewall is an important part of network devices. All the in-bound and outbound traffic is being monitored with the help of firewalls, In ac-chess control, maintaining strong passwords and an authentication mechanism protects the network system from being hacked or data being compromised to an unconcerned person, as well as strengthening the network system's intrusion detection mechanism, which helps to detect real-time illegal traffic and generate an alarm if any unwonted traffic is entered into the system. Encryption of the information: Hiding the IP address: IP address is a key element in network security connection, and the use of proxy server helps to provide extra protection of systems being hacked by using IP logger technology-inquest, use of authentication technology: this technology should be included in verification protocol to secure the information passed through network traffic. Use file encryption: this technique is used to improve the security of system data; data is encrypted using key results that no one can easily decrypt if a hacker gains access to your data [10]. The authors conclude with different security strategies and protection methods of network security.

3. RESEARCH METHODOLOGY

The security of software is particularly concerned, which indicates what type of software security standard should be chosen to be fool-proofed. For software data protection, security is a very critical factor. To develop effective secure software, there are two steps to countermeasure which are as follows:

- Performing Ethical Hacking/penetration testing before the software deployment phase of SDLC.
- Performing Ethical Hacking/penetration testing after the deployment phase of SDLC.

Penetration testers report their test findings to the organization, which is then responsible for making adjustments to either fix or minimize the vulnerabilities. Integrating penetration testing as an important part of the lifecycle of software development implies that your consumers can find the end product safe, secure and stable.

When it comes to software projects, security makes a major difference between success and failure. The objective of this research is to recognize a way to use ethical hacking techniques during the Software Development Life Cycle. We use this technique after the deployment phase of the SDLC model. The study is based on a qualitative approach. The main resource includes research papers, web blogs, and website articles on the subject available.

3.1 Proposed EH-SDLC model

The current research paper will use ethical hacking techniques to ensure the quality of software before and after the deployment phase of the SDLC model. Figure 2 shows our proposed model: Ethical Hacking-Software Development Life Cycle (EH-SDLC).

The main objective was split into the following research questions in order to get a more thorough and in-depth understanding of this subject.

1. Which Operating Systems are useful for finding the vulnerabilities in the software during EH-SDLC?
2. Which tools are useful to test the security of software during EH-SDLC?

Fig. 2. EH-SDLC

1.1 List of Operating Systems are useful during EH-SDLC:

This research presents different operating systems to use in our proposed EH-SDLC model before and after the deployment phase of SLDC. Everything is free, open-source, based on the Linux kernel, and has contained many hacking tools. The main key features of these Ethical hacking operating systems are as shown in table 1.

Table 1. Operating Systems for Ethical Hacking.

Operating systems	Key features
1) Kali Linux[11]	There are over 600 pre-installed penetration testing tools to perform a variety of data security functions, such as Penetration Testing, Security Analysis, Forensics, and Reverse Engineering.
2) Parrot OS[12]	Lightweight with dedicated CDNs. tools such as Anon Surf, Onion Share, TOR, I2P, etc.
3) Back box[13]	The most well-known research techniques, aimed at a broad range of objectives, including web application analysis, network analysis, stress checks, sniffing, vulnerability evaluation, computer forensic analysis, automotive, and exploitation.
4) Black Arch[14]	The repository contains 2668 penetration and security tools. Automation, mobile tools & networking.
5) Fedora Security Lab[15]	Security auditing, forensics, system rescue, and educating on security testing methods.
6) Dracos Linux[16]	Forensics, information gathering & malware analysis. Having three main directories attack, defense and forensics.
7) Bugtraq OS[17]	A wide variety of pen-testing tools, malware tools, and mobile forensic tools.
8) CAINE[18]	Complete Forensic and digital investigation environment.
9) Samurai Web Testing Framework[19]	VMWare supports the Samurai Web Testing Framework as a virtual machine. Perform pen-testing and website attacks tools.
10) Network Security Toolkit [20]	Performs regular security checks and network traffic monitoring tasks. Monitoring of virtual machines on a virtual server.
12)DemonLinux[21]	Hacking tools, VMWare & LIVE with RAM/Squash FS. By pressing just one key, search or open anything.
13) ArchStrike[22]	Pen testing & security layer, open-source tools for investigation.
14) Andrax[23]	Advanced Ethical Hacking and Penetration Testing on Several Platforms, Perform Security Checks on a Variety of Devices (Desktop, Notebook, Android, Raspberry Pi).

1.2 List of Tools are useful during EH-SDLC:

This research presents different tools used in our proposed EH-SDLC model before and after the deployment phase of SLDC.

Table 2. Tools for ethical hacking:

Tools	Key features
1) OWASP Zed Attack Proxy [24]	The most commonly used web app scanner. It's open-source and free.
2) Netsparker[25]	Netsparker is a simple web application security scanner that can detect SQL Injection, XSS, and other vulnerabilities in your web applications automatically.
3) Acunetix[26]	Acunetix is a penetration testing platform that is fully automated. Its web application protection scanner scans HTML5, JavaScript, and single-page applications with pinpoint accuracy.
4) Intruder[27]	The intruder is a robust, automated penetration testing tool that finds security flaws in your IT infrastructure. Intruder protects companies of all sizes from hackers by providing industry-leading security audits, continuous monitoring, and an easy-to-use platform.
5) Indusface[28]	Based on the OWASP top 10 and SANS top 25, Indusface WAS provides manual penetration testing and automated scanning to identify and report vulnerabilities.
6) Intrusion Detection Software-solarwinds[29]	Intrusion Detection Software is a method that can identify a wide range of advanced threats. It offers DSS (Decision Support System) and HIPAA compliance reporting. This framework will keep an eye on suspicious attacks and behavior in real-time.
7) W3af[30]	W3af is a platform for web application attacks and auditing. It has three types of plugins: discovery, audit, and attack, all of which interact with one another to look for any site vulnerabilities.
8) Metasploit[31]	Discover the Remote software vulnerabilities, easily develop and execute exploits, Enumerate and scan the networks and hosts remotely.
9) Nmap[32]	Network mapping and enumeration, Find vulnerabilities of any network.

10) Wireshark[33]	Analyze network traffic, VoIP analysis. captures real-time packets and displays them in a human-readable format.
11) OpenVAS[34]	Detect remote vulnerability of any host computer/server.
12) Iron WASP[35]	Iron WASP is used for web application vulnerability testing
13) Nikto[36]	Scan servers and perform scan tests.
14) SQLMap[37]	Detect different types of vulnerabilities that are based on SQL through SQL code injection tests.
15) SQLNinja[38]	Target & exploit web applications that use MS SQL Server as a background database server.
16) Wapiti[39]	Helpful in finding security flaws in web applications
17) Dradis[40]	Dradis is an open source penetration testing platform. It allows for the preservation of information that can be exchanged between pen-test participants.
18) Ettercap[41]	Ettercap is an all-in-one pen research solution. It is one of the best security testing methods available, and it allows for both active and passive dissection.
19) Burpsuite[42]	It works by intercepting proxy traffic, scanning web applications, crawling content and features.
20) Arachni[43]	Arachni is a Ruby framework-based open source penetration testing and administration tool. It's used to determine how safe modern web applications are.

4. CONCLUSION

To ensure the security quality of software, the most important way is to add Ethical Hacking techniques before and after the deployment phase of the Software Development Life Cycle (SDLC). The majority of the basic operating systems and tools related to ethical hacking are discussed in this paper. This Ethical Hacking-SDLC is essential to keep safeguarding software against hacking attempts. This process reduces the long-term costs that the customer pays if the data breach occurs. The best three advantages of the proposed solution are, improving the overall performance of the software, providing security against threats, and fixing the vulnerabilities present in the system. End-users must be confident that the software development of their product is safe and secure. Our proposed solution of the EH-SDLC model does not guarantee foolproof security protection of software, but it does reduce the chances of threats present in the software. It enhances the chances of success in terms of not only functionality but also efficiency, thus improving the security quality of the overall developed solution.

5. REFERENCES

[1] Luo, C., Bo, W., Kun, H., & Yuesheng, L. (2020). Study on Software Vulnerability Characteristics and Its Identification Method. Mathematical Problems in Engineering, 2020.

[2] "What is Ethical Hacking | Types of Ethical Hacking | EC-Council." https://www.eccouncil.org/ethical-hacking/ (accessed May 11, 2021).

[3] S. Patil, A. Jangra, M. Bhale, A. Raina and P. Kulkarni, "Ethical hacking: The need for cyber security," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 1602-1606, doi: 10.1109/ICPCSI.2017.8391982.

[4] Bertoglio, Daniel & Zorzo, Avelino. (2017). Overview and open issues on penetration test. Journal of the Brazilian Computer Society. 23. 10.1186/s13173-017- 0051-1.

[5] Bacudio, Aileen & Yuan, Xiaohong & Chu, Bei & Jones, Monique. (2011). An Overview of Penetration Testing. International Journal of Network Security & Its Applications. 3. 19-38. 10.5121/ijnsa.2011.3602.

[6] "13 Physical Penetration Testing Methods (That Actually Work)," PurpleSec, Jul. 17, 2019. https://purplesec.us/physical-penetration-testing/ (accessed May 11, 2021).

[7] Mohino, de Higuera, Juan-Ramón & Montalvo, Juan Antonio. (2019). The Application of a New Secure Software Development Life Cycle (S-SDLC) with Agile Methodologies. Electronics. 8. 1218. 10.3390/electronics8111218.

[8] c, Nagadeepa & Mohan, Reenu. (2019). Ethical Hacking: Cyber-Crime Survival in the Digital World. International Journal of Recent Technology and Engineering. 8. 10.35940/ijrte. D4612.118419.

[9] Nishadhi, Nimesha. (2020). Ethical Hacking as A Method to Enhance Information Security. Cyber attack protection methodology.

[10] Shi, Junyan & Li, Juanjuan. (2016). The Security and Protection Strategy Study of Computer Network Information. 10.2991/icence-16.2016.7.

[11] "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution," *Kali Linux*. https://www.kali.org/ (accessed May 10, 2021).

[12] "Parrot Security." https://www.parrotsec.org/ (accessed Mar. 31, 2021).

[13] "Homepage," BackBox.org. https://www.backbox.org/ (accessed May 10, 2021).

[14] "BlackArch Linux - Penetration Testing Distribution." https://blackarch.org/ (accessed May 10, 2021).

[15] "Security Lab." https://labs.fedoraproject.org/en/security/ (accessed May 10, 2021)."Dracos Linux." https://dracos-linux.org/ (accessed May 10, 2021).

[16] "Bugtraq –ArchiveOS." https://archiveos.org/bugtraq/ (accessed May 10, 2021).

[17] "CAINE Live USB/DVD - computer forensics digital forensics." https://www.caine-live.net/ (accessed May 10, 2021).
[18] "Samurai Web Testing Framework – SecTools Top Network Security Tools." https://sectools.org/tool/samurai/ (accessed May 10, 2021).
[19] "Network Security Toolkit (NST 32)." https://www.networksecuritytoolkit.org/nst/index.htm l (accessed May 10, 2021).
[20] "Demon Linux." https://www.demonlinux.com/ (accessed May 10, 2021).
[21] "ArchStrike." https://archstrike.org/ (accessed May 10, 2021).
[22] "ANDRAX Hackers Platform." https://andrax.thecrackertechnology.com/ (accessed May 10, 2021)
[23] "OWASP ZAP Zed Attack Proxy | OWASP." https://owasp.org/www-project-zap/ (accessed May 11, 2021).
[24] "Netsparker | Web Application Security For Enterprise."https://www.netsparker.com/?utm_source=guru99&utm_medium=referral&utm_content=product+description&utm_campaign=generic+advert (accessed May 11, 2021).
[25] "Acunetix | Web Application Security Scanner," Acunetix. https://www.acunetix.com/ (accessed May 11, 2021).
[26] "Intruder | An Effortless Vulnerability Scanner." https://www.intruder.io/?utm_source=referral&utm_campaign=guru99_penetration_testing_tools (accessed May 11, 2021).
[27] "Web Application Scanning (WAS) - Vulnerability Scanning by Indusface." https://www.indusface.com/web-application- scanning.php (accessed May 11, 2021).
[28] "Intrusion Detection Software – IDS Security System | SolarWinds." https://www.solarwinds.com/security-event-manager/use-cases/intrusion-detection-software (accessed May 11, 2021).
[29] "Take a tour | w3af - Open Source Web Application Security Scanner." http://w3af.org/take-a-tour (accessed May 11, 2021).
[30] "Metasploit | Penetration Testing Software, Pen Testing Security," Metasploit. https://www.metasploit.com/ (accessed May 11, 2021).
[31] "Nmap: the Network Mapper - Free Security Scanner." https://nmap.org/ (accessed May 11, 2021).
[32] "Wireshark · Go Deep." https://www.wireshark.org/ (accessed May 11, 2021).
[33] "OpenVAS - OpenVAS - Open Vulnerability Assessment Scanner." https://www.openvas.org/ (accessed May 11, 2021).
[34] "IronWASP: An Introduction - Infosec Resources." https://resources.infosecinstitute.com/topic/ironwasp-part-1-2/ (accessed May 11, 2021).
[35] g0tmi1k, "Nikto." https://tools.kali.org/information-gathering/nikto (accessed May 11, 2021).
[36] "sqlmap: automatic SQL injection and database takeover tool." https//sqlmap.org/ (accessed May 11, 2021).
[37] "sqlninja - a SQL Server injection & takeover tool." http://sqlninja.sourceforge.net/ (accessed May 11, 2021).
[38] "Wapiti : a Free and Open-Source web-application vulnerability scanner in Python for Windows, Linux, BSD, OSX." https://wapiti.sourceforge.io/ (accessed May 11, 2021).
[39] "Dradis Community Edition | Dradis Framework." https://dradisframework.com/ce/ (accessed May 11, 2021).
[40] "Ettercap Home Page." https://www.ettercap-project.org/ (accessed May 11, 2021).
[41] "Burp Suite - Application Security Testing Software - PortSwigger." https://portswigger.net/burp (accessed May 11, 2021).
[42] "Arachni - Web Application Security Scanner Framework," Arachni - Web Application Security Scanner Framework. https://www.arachni- scanner.com/ (accessed May 11, 2021).