The importance of Ethical Hacking tools and techniques in Software Development Life Cycle

Adolfo Cruz

Lusófona University of Porto, Portugal
adolfo00cruz@gmail.com

Abstract. Nowadays developed software can never guarantee to be fully secure against all the type of threats. To help with this task we have ethical hackers who are individuals that are responsible for using different tools and techniques to test the developed software, basically they incorporate the role of bad hackers forcing all the secure parameters of the software but besides of the bad hackers, when they pass through the security firewalls. They don't use the information that they got for something illegal, they just do a document with all the security breaches that the software has and deliver it to the CEO or a superior of the company that they work for. Therefore, the company just tries to find solutions for those breaches.

It's because of this that Ethical Hacking is extremely important for software development, but not just for the company, also for the user's safety (eg. personal data) so investing more in this sector of software development is a must for Internet and Software security around the world.

This research work aims to discuss about several techniques and tools involved in ethical hacking, known attacks and the respective solutions to avoid them on software development security.

Keywords: Hacking, Ethical Hacking, Penetration Testing, Software Security, Software Testing, Software Development, Vulnerability Analysis.

1 Introduction

Millions and millions of euros are lost through mistakes during the Software development process [1]. One of the most expensive mistakes are on the security area of the software (e.g., when the programmers leave security breaches without even knowing it). In case that some company it's hacked besides the economic expense the most crucial problem are the user and company data leaked through the hacking operation because these types of data it´s one of the most valuable for illegal purposes.

To avoid these million-dollar expenses, nowadays, companies contract ethical hackers. How are these individuals? Are people that have skill and knowledge to search and find security breaches on software with many tools and methods.

In this digital life dependency having our information secure and in "good hands" it's crucial. With the result of that we depend on a lot of the ethical hackers and the security of the software that we use in our daily routine.

On this paper it will be explained:
In section 2 "Ethical Hacking" it will be explained what ethical hacking is and who are ethical hackers, the different types of ethical hacking, the phases of ethical hacking and what procedures ethical hackers follow, tools and techniques used by an Ethical Hacker
In section 3 we will analyze Software Development life Cycle and The Secure Software Development Life Cycle, the differences between each other and the advantages of the Secure Software Development Life Cycle.
In section 4 it will be a conclusion based on the research.

2 Ethical Hacking

When we hear the word "hacking" we associate with illegal things.

In other words, when we see a photo of someone with a hoodie and a mask the stereotypical image that comes to our minds it's "Anonymous".

In the end, nothing it's like we think, "hacking" can be on a phrase with a good intention and a random guy with a hoodie and a mask don't exactly as to be a hacker or anonymous.

What is ethical hacking? Ethical hacking it's a penetration testing or pen testing.

The responsible of these penetration tests are called ethical hackers, people with skills and who enjoy a lot learning the details of computer systems and explore their max capabilities.[1][2]

What is the difference between an ethical hacker and a hacker? It's simple, ethical hackers have an attacker's mind but with the intention to help, doing it because they are paid for but in the end the share the security breaches that they found in the respective company that they work for. Bad hackers have the evilest intentions while they are doing an attack, most of the bad hackers do it for money but the difference between this and the ethical hackers it's that the final propose it's with a bad intent, some for being recognized as "heroes".[1]

2.1 Types of ethical hacking

Organizations need to be up to date against every type of hacking attacks because the security that they have can already be outperformed by new hackers' attacks attempts consequently we can use ethical hacking on different situations but let's focus these assessments:

- Infrastructure/Employee
- Application
- Physical Entry
- Stolen Laptop

These assessments could entirely compromise one company, due to the financial costs of the breaches, the leaked information, compromise national security, that's why, once again, ethical hacking should be a must for every company in the software development area.

Infrastructure.

Nowadays this is probably the most dangerous breach that we can have on a company, different policy's have been introduced to prevent attacks by this breach but depends a lot of the company employees.

So, the way that the organization's prevent these attacks are by using a VPN, making a lot of safety policy's to be followed by employees, improving some critical Web Portals safety, … [3]

Ethical Hacking can be useful here by testing employees with Social Engineering and phishing emails to get company information for e.g., and if hackers gain some information by this way, companies can see how far hackers could go with that type of information preventing their following steps by increasing delicate points security. With this, they can be ahead of hackers ideas and prevent future damages to the company not needing to depend on their employees.

Application.

Performing networked-based testing to simulate hackers' behavior on our Web Applications and mobile apps it's another way of improving future damages and losses. It will be helpful ethical hacking this area to test the resilience of the customer portal against unauthorized access or malicious behavior of a valid customer. [3]

2.2 Ethical Hacking Phases

Like one recipe, Ethical Hacking must follow some steps which are: Reconnaissance where the hacker tries to gain information about the target (footprint).
Scanning it's the phase that the hacker use the information of the last step to search vulnerabilities.
Gaining Access where with a list of vulnerabilities the hacker will attack the weak spots.
On Maintaining Access/Zombie System the hacker tries to keep the control of the victim.
The last step will be Evidence Removal that consists in cleaning the proves that the left when attacked.

Reconnaissance.

On this initial step hackers try to gain information of the target, this "information gathering" or "footprint" can be done without knowledge at all from the individual, but it will require much more effort from the hacker to fill all the information gaps, but it can be easily gained too.

There are to types of reconnaissance, active and passive, on the passive the hacker doesn't attack the system or the company network, depends a lot of Social Engineering methods on the target just by searching him on internet or physically getting information (e.g., picking up some target trash that could have vital information), active hacking it's only done when we have information of the target, it's unsafe for the hacker because he can be easily caught, the hacker enters on the company's network to discover individual hosts, network services, and Ip addresses, operating system, etc...

The information gained on this step will be useful on the following step.

Fig. 1. Footprint main information's

Scanning.

Using the information that they get on reconnaissance the hackers now will look at that more deeply trying to find vulnerabilities so they can access the system.

Tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners are used in the scanning phase to scan data and records.

Ethical hacking uses three different methodologies:

- Vulnerability Scanning (find targets vulnerabilities and weak points using Netsparker, Nmap, etc…)
- Port Scanning (opening TCP and UDP ports with port scanners and dialers, finding open doors to access organization's system)
- Network Scanning (find and locates every device connected to the organization network, find ways to exploit the company network)

Gaining Access.

Ethical Hackers will try everything they can, to access the system on an unauthorized way. Every tool and methods will be used to gain access and enter the system, the system can be protected with a firewall and passwords that will slow down the time that a hacker can hack the system.

When succeed, they will be able to exploit the system with malware, steal and leak some sensitive information, infect the system with ransomware. Nowadays the tools that are the most used to do this it's Metasploit.

Maintaining Access / Zombie System.

After having the access ethical hackers will not give that up, so on this step, they will have to maintain the access. Maintaining it will need to launch DDos Attacks, exploit the system, use Trojan tools, steal the entire database, ...

To avoid the system from being exploited, ethical hackers and penetration testers can scan throw the entire company infrastructure to see if it has any malicious activities.

Evidence Removal.

To not get caught the hacker must destroy every evidences and traces of hacking that he did by deleting logs or registry values, uninstalling folders and applications to ensure that everything it's on their original state.

Ethical hackers can erase their tracks:

- Using reverse HTTP Shells
- Erase the digital footprint deleting the cache and history
- Using Internet Control Message Protocol Tunnels

2.3 Tools and Techniques of an Ethical Hacker

Ethical Hackers to do their job use different techniques and tools, these can be used during the SDLC (Software Development Life Cycle).

Table 1. Ethical Hacking techniques

Attacks	Description
Phishing	*Consist on spam emails and bogus websites. To avoid this the company, need to have an anti-phishing detector.*

6

Malware	*We have different types of malware, to avoid them we need to have some program to detect it, dodging future damage.*
SQL Injection	*It's one technique that the main focus it will be the application's database. To avoid this the input never should be used directly on the application code.*
Session Hijacking	*Technique that makes hackers steal our session on the Web Application. To prevent this, we can use secure HTTP or SSL between the application server and the user's browser.[10]*

Table 2. Ethical Hacking Tools

Tool	Description
Metasploit [11]	*Discover vulnerabilities and execute exploits. Enumerate and scan the networks and hosts remotely.*
Nmap [12]	*This tool finds vulnerabilities a network and do a network mapping.*
Nikto [13]	*Scan servers and perform scan tests.*
Wapiti [14]	*Finds security flaws in web application*
Burpsuite [15]	*It works by intercepting proxy traffic and scanning web applications.*

The operating system that Ethical Hackers use more it's Kali Linux [9], because there are 600 pre-installed penetration testing tools. Besides Kali Linux they use also: Parrot OS (tools such TOR and Onion share, lightweight dedicated CDN's), Fedora Security Lab (Security forensics, system rescue and education on security testing methods) , Dracos Linux (has three main directories attack, defense, forensics), Arch Strike (penetration testing, free open-source tools for investigation)

3 SDLC (Software Development Life Cycle)

The SDLC it's a process of developing, implementing, and retiring information systems through a multistep model: Requirement analysis, planning, architectural design, coding, testing and deployment.

It aims to aid developers and other project staff to create a system that meets all technical and user requirements as well as exceeds customer expectations.[16]

On Requirements analysis makes a document that have the expected behavior for the app or software to be developed.

The Planning step it's where the team of programmers, etc.., plan software development calendar.

On Architectural Design the team develops the design for the programmers start developing that on the coding step.

The coding phase it's when the application starts to gain form till the result.

On Testing phase, when the app development it's finished, it is tested for issues like performance, functionality, bugs, security.

Once the application it's tested and has a result, will be deployed in the market.

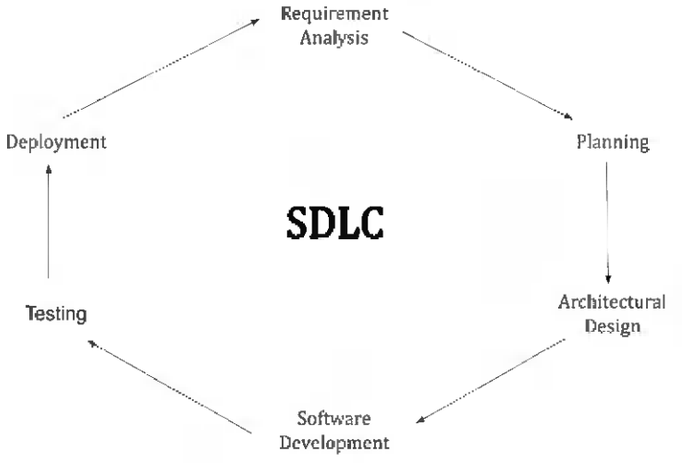

Fig. 2. SDLC steps

As we can see the topic "Security" has been briefly touched on the SDLC, leaving us thinking that the software made it's not secure.

The principal issues caused by this lack of security are: The future costs to resolve the problems ("On average enterprises pay US$551,000 to recover from a security breach. SMBs spend 38K. This is direct spend required to recover from an attack." [17]); The leaked information by cyberattacks, that it's bad to the company and an critical issue to the users because this information gathered by the hackers can have sensitive content ("90% of businesses admitted a security incident. Additionally, 46% of businesses lost sensitive data due to an internal or external security threat." [17]);

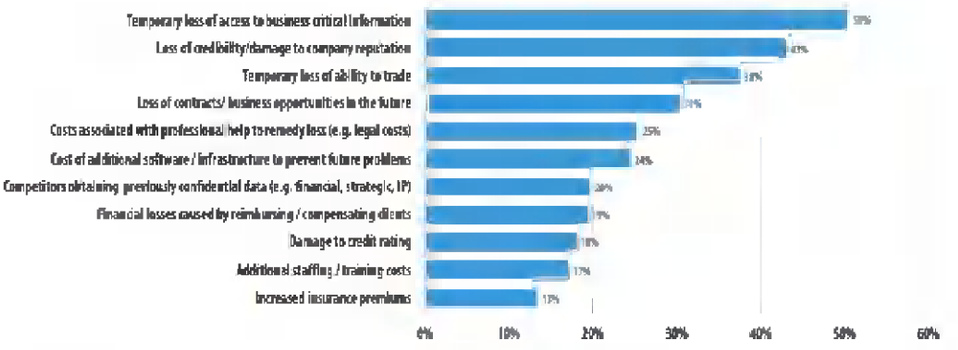

Fig. 3. Frequency of the three worst (chosen by respondents) consequences of a security breaches [17]

The threats experienced by these security and data breaches sometimes are not revealed by the companies, but the ones that revealed said that malware it's most common threat experienced.

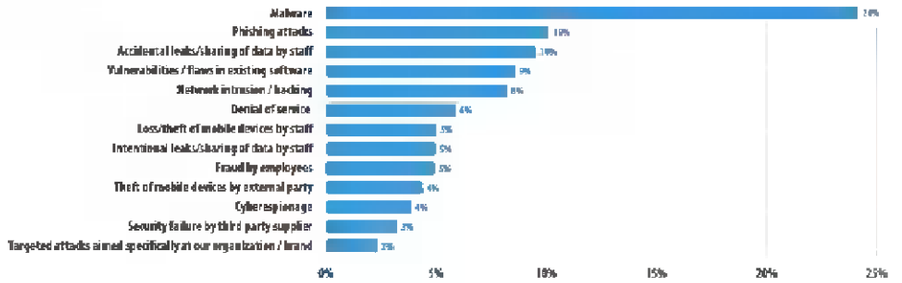

Fig. 4. Threats experienced on companies (chosen by respondents) that are consequences of a security breaches [17]

3.1 Ethical Hacking on SDLC (S-SDLC)

S-SDLC it's an incorporation of the Software Development Life Cycle and security, which means that a software development company can do a better process than the simple SDLC and do a S-SDLC which it's far better on safety. This method because of the security complexity that have made some companies to change their security policy's.

Fig. 5. Representation of a S-SDLC phases

On the requirements phase (after the documentation prepared and approved) it's created the Software Requirement Specification Document or Functional Requirements. These documents contain details of the project such as interfaces, system inputs… The difference between SSDLC and SDLC on this phase it's that here we will have security requirements and Risk Assessment (Strong Authentication, Asset Protection, Supply Chain Security, Data Usage Restriction) [18].

On the Design step we will ensure the security by using for e.g., Cryptosystems (Encryption and decryption of data) and Digital signatures. [19]

Entering the Coding phase, we will have security improvement by doing good coding practices (Error/warning messages, Program organization, clean code) [20].

On the Testing we can use the Fuzzing method that gives us a way of providing invalid inputs to programs to find bugs in software, which can help to find and fix critical bugs. [21]

Finally on the Deployment step we can use for e.g. Server or Network Configuration management that can be summarized as: [22]

- Device hardware and software inventory collection

- Device software management
- Device configuration collection, backup, viewing, archiving, comparison
- Detection of changes to configuration, hardware, or software Configuration change implementation to support change management~

On these phases ethical hackers are crucial and use their techniques to help on the S-SDLC.

4 Conclusion

Technology in the wrong hands can be dangerous and that's why hackers are wrongly misjudge by being only a bad thing to the society. All the news that we saw on TV about Ransomware on a Hospital, Companies getting hacked, etc.... are linked to the word hacker but not with "bad hackers" most people don't know that we have hackers that have good intentions, that help them use some application with more security. These individuals with good intentions are ethical hackers who are professionals that use their hacking skills to improve the security of the apps that we use. Furthermore because of this that Ethical Hacking is extremely important for software development, but not just for the company, also for the users safety (eg. personal data) so investing more on this sector of software development is a must for Internet and Software security around the world.

5 References

1. Luo, C., Bo, W., Kun, H., & Yuesheng, L. (2020). Study on Software Vulnerability Characteristics and It's Identification Method. Mathematical Problems in Engineering, 2020.
2. B. Pandey, L. Balani, A. Singh (2015). Ethical Hacking (Tools, Techniques and Approaches), 2020.
3. Deloitte Ltd (2017). Ethical Hacking Defend against Cyber Attacks. 2017.
4. Danish sharma1,Rituraj Chandra2, C.K Raina3 (2018). Review on Ethical Hacking, 2018.
5. S.Hassan, S.Ahmad (2021). The Importance of Ethical Hacking Tools and Techniques in Software Development Life Cycle (2021).
6. EC-Council. Ethical Hacking and Countermeasures: Attack Phases. vol. 1, EC-COUNCIL | PRESS. 5 vols
7. "Ethical Hacking | Footprinting"shttps://www.geeksforgeeks.org/ethical-hacking-footprinting/.(Accessed December 1, 2021)
8. "What is session hijacking? – Heimdal Security". https://heimdalsecurity.com/blog/session-hijacking/. Accessed 8 December 2021
9. . "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution," Kali Linux. https://www.kali.org/ (accessed December 15, 2021).
10. I. O. Ogundele, A. O. Akinade, and H. O. Alakiri, "Detection and Prevention of Session Hijacking in Web Application Management," International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, no. 7, pp. 1–10, Jul. 2020

11. "Metasploit | Penetration Testing Software, Pen Testing Security," Metasploit. https://www.metasploit.com/ (accessed December 16, 2021).
12. "Nmap: the Network Mapper - Free Security Scanner." https://nmap.org/ (accessed , 2021)
13. "Nikto." https://tools.kali.org/information-gathering/nikto (accessed December 17, 2021)
14. "Wapiti : a Free and Open-Source web-application vulnerability scanner in Python for Windows, Linux, BSD, OSX." https://wapiti.sourceforge.io/ (accessed December 17, 2021)
15. "Burp Suite - Application Security Testing Software - PortSwigger." https://portswigger.net/burp (accessed December 17, 2021).
16. US Department of Justice - The Department of Justice Systems Development Life Cycle Guidance Document. (2003) (accessed January 13,2021)
17. Kaspersky Lab - Damage control: the cost of security breaches, IT security risks special report series. (accessed, January 14)
18. European Union Agency for Network and Information Security ENISA, The EU Cyber Security Agency - Indispensable baseline security requirements for the procurement of secure ICT products and services (December 2016). (accessed 14 January)
19. Le Moyne College INCUBATE (NSF Id 1500033) - Security Design Concepts Target Course: Software Engineering, Software Design. (accessed 14 January)
20. Karl W Broman - Department of Biostatistics Johns Hopkins University (accessed 14 January)
21. Danyang Zhao - Fuzzing Technique in Web Applications and Beyond (accessed 14 January)
22. Cisco Systems, Inc - Network Configuration Management (accessed 14 January)