Information gathering

Pentesting

GCS

Danae Townsend, Jordi Bru, Ignasi Juez, Mariona Jaramillo

March 2023

1.Introduction

a. What is pentesting?

A penetration test, or "pen test," is a security test that launches a mock cyberattack to find vulnerabilities in a computer system.

Penetration testers are security professionals skilled in the art of ethical hacking, which is the use of hacking tools and techniques to fix security weaknesses rather than cause harm. Companies hire pen testers to launch simulated attacks against their apps, networks, and other assets. By staging fake attacks, pen testers help security teams uncover critical security vulnerabilities and improve overall security posture.

The terms "ethical hacking" and "penetration testing" are sometimes used interchangeably, but there is a difference. Ethical hacking is a broader cybersecurity field that includes any use of hacking skills to improve network security. Penetration tests are just one of the methods ethical hackers use. Ethical hackers may also provide malware analysis, risk assessment, and other services. [1]

b. Information gathering and pentesting relationship

Information gathering is the first phase of penetration testing in which we collect publicly available information or internal information about a target while performing active reconnaissance as well as passive reconnaissance. Is the act of gathering information about a system; software service, hardware appliance, network topology, accessible resources, etc. It is also called in his formal definition as Fingerprinting and it is used as a security auditing tool. And all this gathered information can be used in our further testing phases.

There are different roles related to information gathering but not all hacking is unauthorized, and not all hackers break into systems with nefarious aims. Hackers fall into three general categories: black hat hackers, white hat hackers, and gray hat hackers. Although hackers are often associated with exploiting vulnerabilities to gain unauthorized access to computers, systems, or networks, not all hacking is malicious or illegal.

In its purest sense, hacking is simply the application of computer skills to solve a particular problem. There are many different types of hackers, and a lot of hacking activities are beneficial, because they uncover programming weaknesses that help developers improve software products.

1. **White hats**

   White hat hackers also referred to as ethical security hackers who identify and fix vulnerabilities. They have the permission of the victim, organizations the majority of the time to do the penetration testing and try to uncover system weaknesses in order to fix them and help strengthen a system’s overall security.

2. **Black hats**

   Black hat hackers also referred to as malicious hackers are cybercriminals that illegally crack systems with malicious intent. Seeking to gain unauthorized access to computer systems is the definition of black hat hacking. Once a black hat hacker finds a security vulnerability, they try to exploit it and use the information gathered for their own purposes.

3. **Gray hats**

   Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don't have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when gray hat hackers uncover weaknesses such as zero-day vulnerabilities, they report them rather than fully exploiting them.

Purpose of information gathering

The full purpose of information gathering can be broken down to several related objectives:

- It is used to perform security auditing on a system or network.
- Exploit known techniques to better understand a system to then be able to better protect it.
- Obtain a perception on: how is this company regarded from the outside? Provide a report with potential vulnerabilities and attack vectors to a system.

2. Information gathering techniques

a) Active information gathering

Active information gathering is the process of collecting more information about the target network by directly interacting with the target, obviously this is illegal to do without authentication. Active information collection may use, among others, operating system fingerprinting, port scanning, DNS enumeration, etc. We will have an overview of different types of it.

Active fingerprinting is based on performing tasks to obtain as much information as possible regarding the system. The information gathering has the final goal of defining and narrowing down the attack vector. These tasks can be divided into 2 subgroups.

Social tasks where phone calls and work interviews take place and technical tasks where traffic generation and connection “simulation” takes place.

Technical tasks:

Initially we have traffic generation that we can divide into 2 subgroups:

- Packet probing:

  Sending regular traffic with normal applications in order to analyze how the system reacts when receiving the probes.

- Packet crafting:

  Generate special packets to gather as much information as possible. Inspect and modify ongoing (legitimate) packets and analyze the responses as well, you can find a lot of information about how everything works in that site.

Secondarily we have connection simulation:

- We can obtain information with fake connections with particular payloads to trigger errors in the system or to obtain “hidden” information to better understand the system under attack.

Other tasks:

- Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities. It performs a massive test of the list of machines and through well-known TCP and UDP ports. It also permits identifying the attack surface of the victim and it is done by sending SYN packets to a port and waiting for the response. If successful then other traffic may be sent to further identify the application behind the port.
- Banner Grabbing is the term used to refer to the technique of grabbing information of a system available on a certain network and all the services running on its open ports and help out on the forthcoming vulnerability testing through sending simple requests to get welcome information of the services with HTTP requests and checking file extensions.

b) Passive information gathering

In the previous section we discussed one of the information gathering techniques, the active one. And in this one, we will talk about the other side of the coin, the passive, in order to understand its purpose and which resources are usually targeted.

Before continuing, it is important to define the concept of passive information gathering. The key word in this concept is the word "passive", since the objective of this technique is to collect as much information as possible about an organization without it being aware of it [4]. In essence, its purpose is to obtain information that is completely public and probably not directly related to any potential security vulnerability.

In many occasions, the passive information gathering technique during penetration testing and ethical hacking tends to be underestimated, as the emphasis is usually placed on the active technique and vulnerability exploitation. But actually, it plays a great role as it serves to start analyzing the target and see the complexity of the procedure [4].

However, it is important to keep in mind that one of the biggest threats to companies nowadays is unintentionally leaked information, which can be collected without the need to interact directly with the company's servers, which can generate unawareness of possible security breaches [3]. Therefore, it is essential that companies consider this threat and take measures to limit their exposure to potential attacks.

Online resources targeted and tools

As we said before, numerous valuable details can be obtained without any direct interaction with an organization. These details can then be utilized to launch an attack or strengthen other attacks aimed at the objective. Information such as current service patching levels, internal network architecture layout, and account information can be easily acquired from various sources.

The accessibility of online resources plays a vital role in the investigation process. These resources are the following [3]:

- **Internet Service Registration** is responsible for the global registration and maintenance of IP addresses.
- **Domain Name System** manages the local and global registration and maintenance of host naming.
- **Search engines** are used to retrieve distributed material related to an organization or their employees.
- **Email systems** contain valuable information that can be utilized in an attack.
- **Naming conventions** are used by organizations to categorize their online host services.
- **Website Analysis** focuses on information that is intentionally made public but may pose a security risk.

It is also important to be familiar with some of the most common tools used for the passive information gathering phase in order to take advantage of the resources mentioned above.

For DNS related issues [5], tools such as whois (public database for domain information), dig which performs regular DNS queries, fpdns which gathers deep information on DNS and fierce, another more aggressive DNS querying tool, are often used.

In addition, to leverage search engines to their full potential, a tool known as 'The Harvester' is commonly used. As per Kali Linux documentation [5], this tool is designed to gather information about emails, usernames, subdomains, IP addresses, and hostnames from publicly accessible sources, including search engines and websites.

c) Social engineering

Social engineering is another information gathering technique that has a different approach, not so technical as the two mentioned above, but more of a human perspective to determine the level of security robustness of an organization.

To fully understand its purpose, it is important to be aware that technical security measures such as firewalls and intrusion detection systems are essential but can be breached by this technique [6]. These attacks are characterized by exploiting human behavior and psychology, which makes it difficult to defend against them using only technical controls or tools.

This is why social engineering is so important in penetration testing, as it is critical to identify weaknesses in an organization's security awareness, policies and procedures. In addition to making the organization's system security more robust, the results of these tests often help to improve employee awareness of all types of deception, establish more effective security controls, and all with one ultimate goal in mind: reducing the risk of successful cyber attacks.

Types of Social Engineering

Once we have defined the concept of social engineering and clarified its importance in pentesting, we proceed to describe the different types of attacks using this technique that can compromise the security of any organization [9] and every employee has to be aware of.

Phishing

Phishing is a type of attack in which the attacker creates, as an example, a fake web page from an existing one to trick an online user into obtaining personal information. It is a combination of technical and social engineering methods to convince the user to disclose their personal data [7]. This type of attack is typically carried out via email, weblinks and through more creative ones [8].

Categories of Phishing attacks

- **Deceptive Phishing** is a common type of phishing attack where attackers send emails from a recognized sender and add links that imitate legitimate providers to trick users into revealing their personal information.
- **Spear phishing** is a targeted attack where the attacker sends an email from a recognized sender and uses personalized information such as the recipient's full name, title, or position to gain their trust and obtain sensitive information.
- **CEO Fraud**, or whaling, involves attackers using social engineering techniques, such as creating a sense of urgency or authority, to trick executives into revealing login credentials or authorizing fraudulent financial transfers with the intention to steal money or sensitive information from the targeted organization.
- **Vishing** is a type of phishing attack based on voice, where attackers use the phone as the attack vector. The best way to prepare for this type of attack is to avoid answering calls from unknown phone numbers and not provide any personal information.
- **Smishing** is another type of phishing attack that is similar to Vishing, but instead of using the phone as the attack vector, it is based on SMS. The mitigation of it is exactly the same as Vishing.
- **Pharming** is a type of phishing attack that involves redirecting users to a fake website without their knowledge or consent. Attackers use various techniques such as DNS cache poisoning. The goal of pharming is to steal personal information or login credentials from unsuspecting users.

Pretexting

Pretexting is also used to obtain personal information from the victim creating a strong enough pretext or scenario to trick the victim. They may claim to be an authority figure or a trusted entity, and request information to confirm the victim's identity. It is based on requiring some sort of action from the victim to ensure the attack.

Baiting

Baiting is another social engineering attack that involves tempting a victim with something they desire, such as a free gift or information, in order to trick them into revealing sensitive information or performing an action that benefits the attacker. But it is not only with online goods, attackers often use physical objects as bait. For example, CD’s or USB Drives. Curiosity killed the cat, they say.

Quid Pro Quo

This attack operates on the principle of offering something desirable in exchange for information or access. It is similar to baiting, but instead of using a tempting item or information, the attacker promises rewards or benefits to the victim. It often involves the promise of a service or assistance in exchange for the information or access.

Tailgating

Tailgating is a more physical attack in which an attacker gains unauthorized access to a restricted area by following closely behind an authorized person. This attack is also known as the "hold the door" attack, where the actor asks the victim to hold the door for them and gains access to the secured area taking advantage of the victim's tendency to be polite and helpful.

3.Pentesting in companies

a. Overview

As we have introduced previously, the goal of penetration testing is to identify security vulnerabilities that could be exploited by real attackers and to provide recommendations for improving the overall security of the system. Then, there is no doubt that penetration testing can enhance a company's security in many ways:

1. **Identify vulnerabilities via information gathering**: Penetration testing can help identify vulnerabilities in a company's network, software, and hardware infrastructure that could be exploited by hackers. Once these vulnerabilities are identified, the company can take measures to mitigate the risks associated with them.
2. **Test the effectiveness of security measures**: Penetration testing can also help determine the effectiveness of a company's existing security measures. This includes testing the strength of passwords, the effectiveness of firewalls and intrusion detection systems, and the robustness of encryption methods.
3. **Test incident response plans**: Penetration testing can be used to test a company's incident response plans. This involves simulating an attack and observing how the company responds. This can help identify areas where the company's incident response plans may need improvement.

In order to make this become effective, there is the need to provide the root cause analysis of the vulnerabilities identified in a report. This document has to be more business focused around weaknesses in the organization’s global information security strategy, as will be exposed in the section *Reports and security audits* later in this report.

As the information security expert John Yeo well states in his paper named *Using penetration testing to enhance your company’s security, “*any organisation with sensitive information, such as customer data, Personally Identifiable Information (PII), payroll data, payment card data, intellectual property or trade secrets should probably be incorporating penetration testing within their wider governance, risk and compliance activities” [10].

To do so, there are specialist organizations that carry out authoritzed pentesting against networks and applications for many different types of sensitive data. These testings are either conducted at a network general level or at a specific application,

both externally (against Internet-facing servers) and internally (against internal corporate information systems including, for example, servers, workstations and IP telephony systems).

Given that there are lots of laws and regulations regarding hacking, both the tester and the company define which is the specific target system to be pentested. The limits of systems that can be subjected to penetration testing are typically defined by companies based on various factors, including:

- **Legal and ethical considerations**: Testers must work closely with the company to determine which systems can be tested and the scope of testing that is permitted. They should also follow all legal and ethical guidelines to ensure that testing is conducted safely and responsibly.
- **Business-criticality**: Companies may also consider the business-criticality of a system before allowing it to be penetration tested. Business-critical systems, such as those that store sensitive customer data or process financial transactions, may require more stringent security measures and testing procedures to ensure they remain secure and keep working.

b. Teams

Different teams are needed in order to conduct the penetration testing. In this section we will talk about the most important ones, these are: red and blue teams.

While a red team is a group of professionals who simulate real-world attacks on a company's systems and networks to identify potential vulnerabilities; a blue team, on the other hand, is responsible for defending the organization's systems against attacks: they work to monitor the network and identify potential threats before they can cause any harm.

The two perspectives are linked because threats identified by the Blue Team can be tried to be exploited by the Red Ream when carrying out pentesting. Then, a combined Red and Blue Team Methodology often concludes in better results because it aims to provide information on both exploitable means and defensive strategies. In the next schema, the red and blue team combined methodology is graphically clarified.

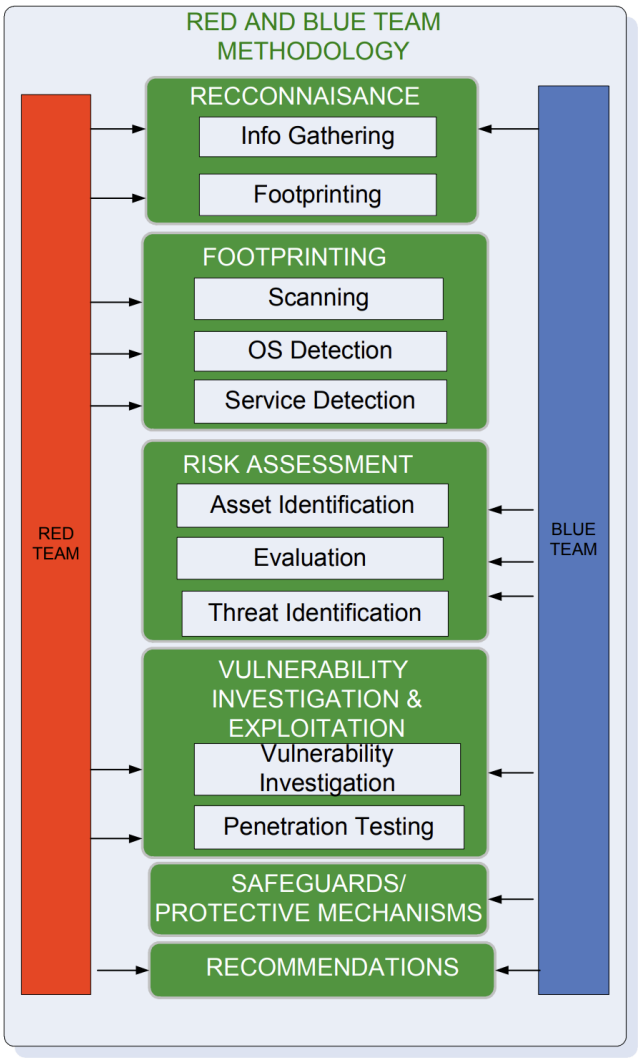

Figure 1. Red and blue team methodology.

Source: N. Veerasamy, "High-Level Methodology for Carrying out Combined Red and Blue Teams," 2009 Second International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 2009, pp. 416-420, doi: 10.1109/ICCEE.2009.177.

It is important to note that information gathering is a technique that is used in both Red and Blue teams given that it gives details about the target and approaches of manipulation impact.

Actually, each security audit starts with an attempt to gather as much information as possible on the subject of interest. During this information gathering process, details such as the IP range, configuration settings and applications can be revealed and used by the Red Team to interact with the system and networks. Moreover, information such as policy compilation and conformance can be useful to gather for the Blue Team. All together, information gathering helps describe the current status and problems. As N Veerasamy defends in the paper titled *High-level Methodology for Carrying out Combined Red and Blue Teams* [11], information gathering can be carried out in several ways in a company by Red and Blue Teams and is divided into

1. **Briefings and meetings:** it serves to provide the team members with contextual information prior to the execution.
2. **Interviews:** these are carried out with personnel members like users, administrators, managers, etc. to have a general understanding from all the operation levels.
3. **Document reviews**: consists in reviewing security policies, operational guidelines and previous assessments to see which is the current level of security.
4. **Internet and search engines:** as websites have lots of information, it is crucial to see if systems configurations are secure enough
5. **Network mapping:** to visualize the network and obtain the default number of users and devices.
6. **Port scans:** it is important to identify active devices, which can become possible targets to be exploited.
7. **Wireless scanning**: once users add wireless accekss points, they could potentially open the network for unsecured access by remote users and this could lead to security breaches. Then, wireless scanning becomes very important in terms of identifying potential attackers and block or prevent them from pursuing these attacks.
8. **Risk assessment**: a risk study gathers information to identify possible threats and assesses critical resources. It is often done by the Blue Team.

c. Reports and security audits

A penetration testing report must provide clear and detailed information on identified vulnerabilities and recommendations for their respective solutions. Performing the technical evaluation report is the fundamental component of the overall evaluation process. The outcome is the production of a written and informative report that is easily comprehensible, whose most notable purpose is to highlight the risks encountered during the evaluated phases. This report must be read by the executive management and technical staff to apply the appropriate measures.

As detailed by Sean-Philip Oriyano in his book "Penetration Testing - Essentials," [12], the most significant topics that should be included in a report are:

- Results of the process and established objectives
- Methodology
- Identified vulnerabilities
- Exploitation of vulnerabilities
- Recommendations

Additionally, any relevant documentation requested by the company can also be included.

a. Results of the process and established objectives

The purpose of this executive summary of the report is to provide company executives with a clear and concise understanding of the following:

- The purpose of the test and the business needs behind it.
- A description of how the tests enabled the organization to understand its systems.
- The key findings focused on a commercial level. Problems that influence the reputation of the client company should be included. Description of technical details should be avoided as the purpose is to understand the commercial impact.
- Strategic recommendations to avoid resorting to repeating mistakes. The writing should avoid technical terms.

The summary will be characterized by being positive, significant, and constructive. Negative aspects should be avoided. The inclusion of figures and graphs is necessary to support and clarify the message to be given.

b. Methodology

In this section, the methodology that was used to perform the pentesting should be listed. An example of the methodology can be found in the Penetration Test Execution Standard (PTES), which is known for being a common framework that establishes a set of guidelines and procedures for the planning and execution of tests. The phases include: preparation, information gathering, vulnerability detection, exploitation, post-exploitation, results analysis and reporting [13].

c. Identified and exploitation of vulnerabilities

For each vulnerability, the description of the root of origin, the impact and the probability of occurrence must be shown. Within the impact, the exploitation of vulnerabilities caused by the process agent must be explained, while the probability of occurrence will be linked to the level of risk, which will allow managers and technicians to know the order of priority and urgency in which it must be applied and handle vulnerabilities [14]. In addition, detailed steps for solving the finding should be included, including suggestions and improvements that could be implemented in the company by the IT team.

The reports and results of the security and pentesting tests carried out will be documented depending on the target personnel, which includes the CIO, CISO and ISSO of the company. In the same way, program administrators or system owners should also be listed in the target staff. This is due to the variety of audiences, so the report must satisfy and ensure that each of the personnel involved is properly approached.

d. Tools

The diversity of tools for the execution of a pentesting is wide. In the case of web application scanners, they are presented as automated tools called Dynamic Application Security Testing Tools (DAST), which are responsible for looking for vulnerabilities such as: SQL injection, command injection, insecure server configuration or traversal path. [15].

a. Purpose

The purpose of using the tools is related to vulnerability scanning, reception and extraction of data from a specific network, packet capture and access to the database. [16]

b. General tools

Some of the best known tools include: Acunetix, Wapiti, Arachni, Burp Suite, Netsparker, Vega, SQLMap and ZAP.

c. Recommended vulnerability scanning tool: Acunetix

Acunetix is known for being a tool used to audit web applications finding hard-to-detect vulnerabilities due to the use of Accusor. It is worth noting the internal use of DeepScan technology, allowing interaction with complex technologies such as AJAX, SOAP/WSDL, JSON, Google web Toolkit and CRUD operations, this significantly increases the coverage of the scanner performed. Within its documentation it provides case studies recognized by different companies worldwide [15].

Rank	Detection Accuracy	Vulnerability Scanner
1	94%	Acunetix
2	91%	Netsparker
3	44%	Wapiti
4	19%	Arachni
5	16%	Burp Suite Professional

Figure 2. Score of Web Application Scanner [d-5].

Source: https://owasp.org/www-community/Vulnerability_Scanning_Tools

d. Recommended tool for database penetration testing: SQL Map

SQL Map is an Open source tool whose purpose is intended for the penetration of databases, supported by most of them. It allows the recognition of characteristics of the hosted information, flexibility in data management and also to execute commands maintaining a stable connection along with a friendly and interactive user interface [17].

e. Recommended tool for packet capture: Burp Suite

It is an advanced level tool for the personalized attack of web applications. Its use lies in finding vulnerabilities and obtaining confidential data. In general, the result is obtained faster using Burp suite than manually, while improving accuracy.

4.Conclusions

In conclusion, information gathering is the base and first phase in the penetration testing stages as we have seen in this report. It involves collecting data about the target system, network, or application, which can help identify vulnerabilities and potential attack vectors. The success of a pentesting engagement depends heavily on the quality and accuracy of the information gathered during this phase. Effective information gathering requires a combination of technical skills, creativity, and patience.

Moreover, different tools and techniques can be used to gather information, such as passive reconnaissance, active reconnaissance, and social engineering. The choice of the appropriate methods and tools depends on the scope and objectives of the pentesting engagement.

In summary, information gathering is a critical aspect of pentesting that helps identify potential vulnerabilities and weaknesses that can be exploited by attackers. Therefore, it should be performed thoroughly and systematically to ensure a comprehensive and accurate understanding of the target system or network.

5.References

[1] IBM, Penetration Testing [Online; accessed 4th April 2023 https://www.ibm.com/topics/penetration-testing]

[2] Jedi-Cybersecurity-course-slides

[3] G. Ollmann, "Passive Information Gathering Part 1: Introduction to Passive Information Gathering," Technical Information [Online; accessed 4th April 2023 http://www.technicalinfo.net/papers/PassiveInfoPart1.html]

[4] A. S. Laxmi Kowta, K. Bhowmick, J. R. Kaur and N. Jeyanthi, "Analysis and Overview of Information Gathering & Tools for Pentesting," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-13, doi: 10.1109/ICCCI50826.2021.9457015

[5] Kali Linux. (n.d.). Tools. [Online; accessed 4th April 2023 https://www.kali.org/tools/]

[6] Z. Wang, H. Zhu and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," in IEEE Access, vol. 9, pp. 11895-11910, 2021, doi: 10.1109/ACCESS.2021.3051633

[7] S. Gupta, A. Singhal and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 537-540, doi: 10.1109/CCAA.2016.7813778

[8] “6 Common Phishing Attacks and How to Protect Against Them", Tripwire, 01-Jul-2019. [Online; accessed 4th April 2023 https://www.tripwire.com/state-of-security/6-common-phishing-attacks-and-how-to-protect-against-them]

[9] "5 Social Engineering Attacks to Watch Out For", Tripwire, 07-Jun-2019. [Online; accessed 4th April 2023 https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/]

[10] Yeo, John. (2013). Using penetration testing to enhance your company's security. Computer Fraud & Security. 2013. 17–20. 10.1016/S1361-3723(13)70039-3

[11] N. Veerasamy, "High-Level Methodology for Carrying out Combined Red and Blue Teams," 2009 Second International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 2009, pp. 416-420, doi: 10.1109/ICCEE.2009.177

[12] S.-P. Oriyano, Penetration Testing - Essentials. Indianapolis, Indiana: Sybex, 2017.

[13] "Reporting - The Penetration Testing Execution Standard". The Penetration Testing Execution Standard [Online; accessed 4th April 2023http://www.pentest-standard.org/index.php/Reporting#Report_Structure]

[14] M. Alharbi, "Writing a Penetration testing report", *SANS Inst.*, vol. 1, pp. 8–13.

[15] "Vulnerability Scanning Tools | OWASP Foundation". OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation [Online; accessed 4th April 2023 https://owasp.org/www-community/Vulnerability_Scanning_Tools]

[16] M. Turuvekere y A. A., "A Comparative Study of Pen Testing Tools", *Int. J. Comput. Appl.*, vol. 179, n.º 50, pp. 26–30, junio de 2018 [Online; accessed 4th April 2023 https://doi.org/10.5120/ijca2018917318]

[17] "Case Studies Archive | Acunetix". Acunetix [Online; accessed 4th April 2023 https://www.acunetix.com/case-studies/]

[18] "sqlmap: automatic SQL injection and database takeover tool". sqlmap: automatic SQL injection and database takeover tool. [Online; accessed 4th April 2023 https://sqlmap.org/]