Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Adopting Automated Penetration Testing Tools: A Cost-Effective Approach to Enhancing Cybersecurity in Small Organizations

Yazeed Alkhurayyif*, Yazeed Saad Almarshdy
Department of Computer Science, Shaqra University, Shaqra, Saudi Arabia.

Received 18 Jan. 2024; Accepted 10 May. 2024; Available Online 24 Jun. 2024

Abstract

Modern society is heavily reliant upon the internet. Accordingly, it is vital to ensure that the data transmitted over the internet is safe. Several tools have been created for cybersecurity experts and organizations to test the security levels of organizational networks and websites. However, due to financial constraints, small organizations need to pay closer attention to managing data with limited resources. This study explores the role of automated penetration testing tools in providing small organizations with an effective and affordable data security system. This study employs a case-study approach using multiple data-gathering methods in a charitable organization. More specifically, data was collected using interviews and experiments evaluating penetration testing tools. The results revealed that cost-effective automated penetration testing tools could safeguard small organizations from cybersecurity threats. The penetration testing tools determined that the organization's website had various vulnerabilities. The Nessus tool discovered no fewer than 37 vulnerabilities on the website application. The ZAP testing tool showed that the website application was critically failing, leading to the accumulation of vulnerabilities. The system had 3 medium-, 12 low-, and 4-informational-risk vulnerabilities. Through the evaluation of open ports, the NMAP tool identified various vulnerabilities. These findings have important implications for small organizations. First, automated penetration testing tools can be easily conducted by small organizations to safeguard their cybersecurity without obtaining costly expert help. Second, it is recommended in the light of the findings that automated penetration testing tools be used in multiple combinations as different tools have unique contributions to cybersecurity.

I. Introduction

In the ever-growing world of technology, the internet has been indelibly intertwined with the daily lives of human beings [1]. In the 21st century [2], information, communication, and data storage have been disseminated virtually through the Internet. This has created a need to ensure that transmitted information remains secure. For instance, with the advent of mobile banking [3], virtual transactions at the touch of a button have been made possible. However, given the network infrastructure, hacking into these systems is relatively easy. This has created a growing need to ensure cybersecurity—especially for critical areas that disseminate sensitive information—and to protect the users of computer

Keywords: Cyber-attacks, Cybersecurity, Penetration testing, Small organization

Production and hosting by NAUSS

* Corresponding Author: Yazeed Alkhurayyif
Email: yalkhurayyif@su.edu.sa
doi: 10.26735/RJJT2453

infrastructure and network systems [4]. This study seeks to identify the roles of automated penetration testing tools in small organizations. Penetration testing makes possible the simulation of the different methods that hackers may use to breach a system [5]. Therefore, by using the Open Web Application Security Project (OWASP) guidelines [6], one can guarantee that all necessary security needs are met. Accordingly, penetration testing allows one to examine a system's security, and evaluate possible measures for enhancing the system network through hardware and software improvements, and make recommendations.

A. Statement of the Problem

Previous studies [5],[6] have indicated that, between 2017 and 2021, the world's global economy has incurred over one trillion dollars in losses due to cybersecurity attacks. These losses have heightened concerns over the security of network and computer infrastructure systems [7]. However, according to the same report, the increased cost of penetration testers and the scarcity of professionals have become a huge barrier to ensuring the security of one's information online. There is significant demand for cybersecurity specialists in the United States, with NIST (2018) proposing to hire over 300,000 new workers, up from the present total of over 700,000. Small organizations may not be financially privileged to hire a sufficient number of cybersecurity specialists to safeguard themselves from cybersecurity threats. It would be good news for small organizations if automated penetration testing tools, which are affordable, empirically proved to be effective in increasing their cybersecurity. Furthermore, it would be a good contribution if the relative effectiveness of various automated penetration testing tools were determined. Accordingly, this paper addressed the following questions:

1) Are automated penetration testing tools effective in evaluating the security of small organizations?
2) Which automated penetration testing tools would be most effective in securing small organizations?

B. Research Objectives

This research aims to examine the role of automated penetration testing tools in small organizations for the provision of effective and affordable security, which would allow such organizations to evaluate risks, increase security levels, and protect sensitive information. The following objectives have been set:

- Explore the role of automated penetration testing tools in small organizations to increase their security without inviting huge expenditures for hiring penetration testers.
- The provision of effective and affordable security, which would allow such organizations to protect their sensitive information, assess risk, and increase security levels.
- Determine which of these tools is more efficient and economical for small organizations through experimentation.

The remaining part of the paper is organized as follows: in section II, the author presents the theoretical background of the importance of cybersecurity, and penetration testing. Section III discusses the methodology of the proposed study. The results and discussion are presented in section IV. Finally, section V concludes the study with its limitations and future directions.

II. Background

A. The Importance of Cybersecurity

Cybersecurity protects information systems from harm purposefully caused by the operator or by the accidental failure to adhere to security measures [8, 9]. Awareness of cybersecurity is important for both individuals and businesses. If information is stolen from personal devices, hackers may use your information to attack those closest to you, leading them to be fleeced of their hard-earned money. One of the most well-known examples of social engineering cyberattacks occurred in Germany in December 2014 [10]. By sending targeted phishing emails that seized a user's credentials, the hackers gained access to the servers causing severe financial and production losses to the manufacturing facility.

A spear-phishing email attack cost Ubiquiti Net-

work, a networking equipment company based in San Jose, California, $46.7 million, of which only a fraction was recovered. In both cases, the attackers capitalized upon human flaws to wreak cyber harm. Cybersecurity is a broad term with many different definitions. Three key ideas are essential to the understanding of the term "cybersecurity," which are [10]:

- Confidentiality: The process of limiting access to information. This security measure entails setting strong passwords to protect important accounts [23].
- Integrity: This process ensures that system data is verifiable, accurate, and trustworthy. As such, one cannot change, destroy, or access specific data without authorization from the system administrator. Cybersecurity thus aims to provide better accountability and control over user access. Having a secure backup is another important component of data integrity. Cloud backups are currently one of the most dependable choices.
- Availability: This process is crucial since it ensures that the system functions smoothly and that data can be accessed without delay. Availability thus refers to the continuous upgrade and maintenance of the system. In the fight against cyberattacks, firewalls, proxy servers, backup systems, and disaster recovery plans are all essential tools.

B. Penetration Testing

Penetration testing is a method whereby individual binary components or entire applications are tested to see whether intra- or inter-component vulnerabilities may be exploited to compromise the app, its data, or its environmental resources. Due to the complexity of computer systems, creating and maintaining an accurate model of how potential exploitation will affect any specific system is a huge difficulty for penetration testing [7], [11], [32].

Most hacking tools target operating systems, applications, Shrink-Wrap Code, or misconfigurations [11], [32]. Many system administrators leave default settings while installing operating systems, resulting in potential vulnerabilities remaining unpatched. For applications, when developers write code, applications are not always adequately tested for vulnerabilities, which can lead to a slew of programming errors waiting to be capitalized upon by hackers. The majority of application development is "feature-driven," which means that programmers face increased pressure to produce quality products in the shortest possible time. Shrink-Wrap Code is often targeted as many off-the-shelf programs have hidden features that the average user is unaware of and could easily be exploited. For example, macros in Microsoft Word can allow a hacker to run programs from within the program. Misconfigurations are targeted as they make things easier for the user; systems can be misconfigured or left at the most basic security settings, leading to vulnerabilities and attacks [33].

C. Objectives of Penetration Testing

As computer systems evolve further and improve their capabilities in many aspects of our lives, the need to safeguard these systems grows in lockstep. A penetration test provides a bird's-eye view of an organization's IT infrastructure's current security posture [25]. The process entails a thorough examination of the system for any potential vulnerabilities that may arise due to inadequate or incorrect system configuration, known and/or unknown hardware or software defects, or operational flaws in the process or technical countermeasures. It aids in reducing security risks and determining the efficacy of current security measures. Penetration testing should be further adapted due to its being a good first step in understanding an organization's current security posture by identifying flaws and security breaches, as well as in locating where suitable actions should be applied in order to mitigate any potential threats.

Furthermore, it allows for the identification, understanding, and prioritization of security risks, as well as an assessment of their impact and, in many cases, a mitigation strategy. Additionally, these initiatives may result in more effective budget allocation for information security concerns [34]. It is also advantageous because it allows organizations to heighten the security of their firewalls, routers, and servers. Data can also be secured through several

security measures, such as intrusion detection systems, firewalls, and cryptography.

Penetration testing can also improve the security of an organization's overall infrastructure. In addition to testing technical infrastructure, the test also assesses management and employee infrastructure [35]. Penetration testing is also helpful when conducting due diligence and independent audits. An unbiased security analysis and penetration test can direct internal security resources to the most critical areas. Furthermore, an independent security audit provides evidence of due diligence in a legal framework for safeguarding online assets, thereby reducing the risk of shareholder value loss. Moreover, independent audits are increasingly required for obtaining cybersecurity insurance. Penetration testing thus provides important validation feedback between business efforts and a security framework, allowing for the mitigation of risk and financial loss [34].

D. Common Penetration Testing Tools

Penetration testing techniques are used to analyze a network's protection mechanisms and security rules, as well as OSs, services, applications, and even end-user behavior. Penetration testing is a type of software testing that looks for vulnerabilities and security problems [8].

1) Network Mapper (NMAP)

For most security professionals [24], NMAP is a free, open-source, and strong application. NMAPs are applications with increased scalability and capacity to identify network hosts. The application is also capable of determining the services provided, the OSs that are running, and the packet filters/firewalls in use. NMAP returns a list of scanned targets, along with supplementary information based on the choices selected. The port table contains the most important information, including port numbers, protocols, service names, and states. There are four possible states for network ports: open, filtered, closed, and unfiltered. Open indicates that the target host is listening for connections/packets on a particular port. Filtered indicates that the port is blocked by a firewall, filter, or other network impediments, thus preventing one from determining whether it is open or closed. There is no application listening to closed ports, although they can open at any time. Ports are classified as unfiltered when they are responsive to NMAP's probes, but the app cannot determine whether they are open or closed. Below is a brief outline of some of the most important NMAP options [15]. NMAP can help fulfill controls for SOC 2, ISO 27001, HIPAA, and PCI [30].

2) HPING

HPING is a utility that extends the standard ping capabilities by allowing users to produce bespoke IP packets for security audits and testing. Port scanning is one use of HPING [11]. Moreover, HPING also provides access control and firewall testing. It can be used to test firewall rules. It also allows for network protocol testing and can be used to craft any packet to test how the system responds to malformed communications [25]. HPING can help fulfill controls for ISO 27001, SOC2, and NIST Cybersecurity framework [30].

3) HARVESTER

External pen testing is made easy with the Harvester, a command prompt tool. It is a Python utility for quickly sifting through a customer's online footprint. It can collect data on emails, subdomains, hosts, employee names, open ports, and banners from a variety of public sources, such as search engines, PGP, LinkedIn, and Twitter [10]. HARVESTER can help fulfill controls for NIST Cybersecurity Framework, and GDPR [31].

4) WIRESHARK

WireShark is an open-source network packet analyzer or software that captures and attempts to display packets from a network. It can be used to examine network protocols, troubleshoot new protocols, investigate network problems, and uncover security risks, among other functions. Listening to network traffic might identify security weaknesses or serve as a foundation for many types of attacks. For instance, clear-text data supplied to apps from web forms or services can include sensitive information or highlight a lack of input validation. Wire-

shark can also be used to examine the protocols used by various machines as they communicate over a network, thereby identifying inconsistencies that can be exploited [11], [18]. WireShark can help fulfill controls for IEEE 802.3-2005 [31].

5) NETCAT

Netcat is a networking utility for working with ports and performs such tasks as port scanning, listening, and redirection. This command is also useful for debugging and testing network daemons. This gadget is known as the networking equivalent of the Swiss army knife. It could also be used to perform TCP, UDP, or UNIX-domain socket operations, as well as open remote connections, and much more. Kali Linux comes with Netcat pre-installed [18]. NETCAT can help fulfill controls for ISO 27001 [30].

6) OWASP ZAP

The Open Web Application Security Initiative (OWASP) is an open-source project dedicated to web application security [15, 26]. Its goal is to make software security more transparent in order to enable individuals and businesses to make educated decisions. The basic purpose of ZAP is to simplify the penetration testing of online applications. ZAP is advantageous in that it provides a cross-platform capability, i.e., it works across all OSs (Linux, Mac, Windows, etc.), is reusable, can generate reports, is ideal for beginners, and is offered at no extra cost. OWASP ZAP can help fulfill controls for SOC 2, ISO 27001, HIPAA, GDPR, and PCI [30].

7) ARJUN

Arjun is a tool that may be used to find hidden URL parameters that are present on a given URL address. It is written in Python. Available parameters are found using two methods: Checking for HTML elements that could be related to parameter names and brute-forcing the parameters using a list of well-known URL parameters. First, the URL of the target application is queried without any additional parameters and the answer is logged. Next, a six-character pseudo-random string is constructed and used as a dummy parameter for the target URL (under the assumption that this parameter does not exist on the target application), a fresh request is submitted, and the response is re-evaluated. HTML elements, such as form and input, are searched for during the first response analysis, and their properties are evaluated for probable parameter names. If the parameters are discovered, they are added to a list of parameters that Arjun will subsequently fuzz. The application examines whether the pseudo-randomly generated string supplied as a parameter exists and whether its name or value was reflected in the response while evaluating the second request. The response codes of both requests are then compared. In so doing, Arjun learns how the target application responds when given a non-existent parameter. Arjun begins creating and sending further requests to the target application's URL with added parameters based on the list of well-known URL parameters, as well as the available parameters derived from the first request's response after the initial requests have been made and processed [23]. ARJUN can help fulfill controls for ISO 27001 [30].

8) NESSUS

Originally open source but is now a proprietary cross-platform vulnerability scanner [11], Nessus was developed by Tenable Network Security with client/server architecture. The Nessus server performs the actual scanning activity, while the client remains at the front-end application of the program. Both clients and servers can be installed into a single system or on separate machines. The Nessus pentation testing tool's key feature is the scan policy, which permits the user to set parameters and variables for a successful scanning, such as scan options, credentials, plugins, and advanced settings. It is used to detect potential vulnerabilities and weaknesses in the network and systems, such as remote cracker control, default passwords, DoS attacks, missing updates, and patches by using an up-to-date security vulnerability database [11]. Scanning a system or a network is simple using Nessus. The configuration of policies to examine the system or network after logging into the online portal is made possible through thousands of plugins that detect vulnerabilities, which thus provides ample intelligence for evaluation. After policies have

been configured, the next step involves selecting the device's IP address or range of the network that will be assessed. Once the targets have been selected, a scan can be launched, and Nessus will start its vulnerability analysis. Once scan is performed, Nessus presents a list of discovered items that can be browsed by severity level. The severity level is ranked by Nessus using a critical, high, medium, low, and info scale. A full explanation of each vulnerability is also provided, as well as a complete downloadable report in a variety of formats to incorporate the vulnerability. Without a plan, a penetration tester should not run Nessus against the entire organization's address range and expect to receive anything useful. Because some plugins are potentially disruptive and can cause many problems, one should proceed with caution. NESSUS can help fulfill controls for SOC 2 and PCI [31].

9) KALI LINUX

Kali Linux is a free and open-source security OS based on the Linux kernel. This package includes a vast collection of auditing and exploitation tools. The distribution was created with forensics and penetration testing in mind. The distribution is available in a variety of formats, including a Live CD, an installable source, and a virtual image [25]. Kali Linux can help fulfill controls for: SOC 2, ISO 27001, HIPAA, GDPR, and PCI [30].

10) BURP SUITE

Burp Suite is a tool for evaluating the security of online applications and can map and analyze an application's environment. A Repeater, a Decoder, a Sequencer, a Comparer, Burp Intruder, HTTP(s), and WebSocket's proxy are all included in the Community Edition [25]. This tool is one of the most popular among professional testers due to the numerous plugins and functionalities it offers. Burp Spider is a tool for web application crawling, which refers to the automatic and methodical browsing of an online application with the goal of creating a full map of the program. BURP SUITE can help fulfill controls for ISO 27001 [30].

11) TCPdump

TCP dump is a command-line network that is a tool for analyzing and examining network data. It can intercept and show data packets on the network interface of your Linux/UNIX system in actual time [29]. TCPdump can help fulfill controls for ISO 27001 [30].

E. Types Of Penetration Testing

In order to stress-test the efficiency of security mechanisms, penetration testing aims to identify faults or vulnerabilities in systems, networks, human resources, or physical assets. The type of penetra-

TABLE I
COMPARISON OF THE INTRODUCED PENETRATION TESTING TOOLS

Tool	Type	Purpose	Compliance Reporting
NMAP	Free	Port Scanner	SOC 2, ISO 27001, HIPAA, and PCI
HPING	Open Source	Network Testing	ISO 27001, SOC2, and NIST Cybersecurity framework
HARVESTER	Open Source	Command prompt tool	NIST Cybersecurity Framework, and GDPR
WIRESHARK	Open Source	Packet Analyzer	IEEE 802.3-2005
NETCAT	Free	Network Testing	ISO 27001
OWASP ZAP	Open Source	Web application auditing	SOC 2, ISO 27001, HIPAA, GDPR, and PCI
ARJUN	Open Source	Finding hidden URL parameters	ISO 27001
NESSUS	Commercial	Vulnerability Scanner	SOC 2 and PCI
KALI LINUX	Open Source	OS containing open source tools	SOC 2, ISO 27001, HIPAA, GDPR, and PCI
BURP SUITE	Commercial	Web application auditing	ISO 27001
TCPdump	Open Source	command-line packet analyzer	ISO 27001

tion testing used is typically determined by the project's scope and the organization's needs [20].

Fig. 1 presents the most common types of penetration testing. These include lack Box Penetration Testing, White Box Penetration Testing, Grey Box Penetration Testing, social engineering attempts, and Red/Blue/Purple team engagements [23].

F. Benefits of Penetration Testing

Penetration testing has numerous advantages on both business and technical levels. The following are some of the most compelling reasons for using penetration testing [20]:

- Security Issues: Malware attacks, network intrusion, and data theft are all security issues that can cause service interruptions and unreliable system procedures. These intrusions may result in a loss of consumer loyalty and impact the company's market value. Penetration testing can help prevent this by screening out both persistent and unexpected threats.
- Protecting information: Access control measures, firewalls, cryptography, intrusion detection systems, and other security procedures are used by businesses to protect information. However, with new attacks being discovered daily, it is challenging to maintain constant protection of user/system information. By simulating a range of attacks simultaneously, penetration testing could address these problems.
- Prioritizing security risks: Penetration testing as a regular security practice not only assists in the understanding of security vulnerabilities but also helps in the prioritization of these issues. The severity of the concerns discovered during the testing can be prioritized. Additionally, these initiatives may result in more effective budget allocation for information security concerns.
- Financial Loss: Penetration testing helps to reduce revenue/capital losses caused by malicious attacks by reducing service downtime. It can also help avoid or decrease fines and lawsuits due to security breaches.
- Guaranteeing Trust: Security breaches are risky for businesses because they might expose confidential information or result in financial losses, which can upset customers. Organizations can ensure clients of complete safety and security through penetration testing. This helps to maintain a company's image and reputation, which in turn increases client trust.
- Hackers' method exposed: Penetration testing tools and strategies evolve at the same rate as hacking methods to ensure that security is always up to date. Penetration testing helps to constantly disclose different ways to hack systems so that corporations know the security improvements required to prevent such attacks. Organizations must use penetration testing to expose hackers' methods to stay one step ahead.

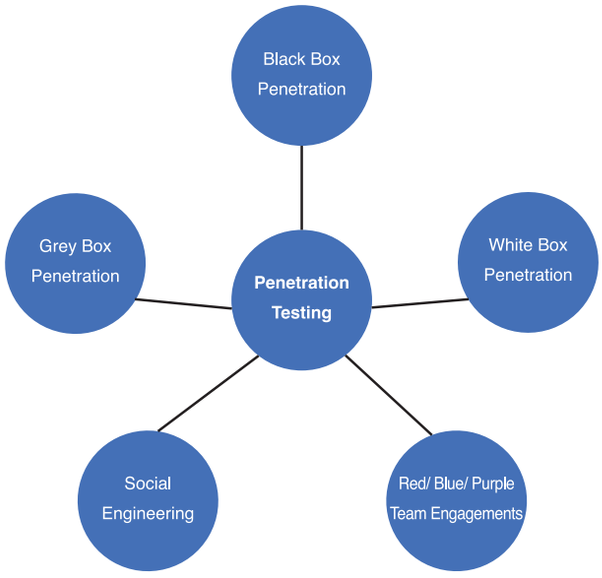


Fig. 1. Penetration Testing Types.

G. Penetration Testing Process

Penetration testing can be divided into several sections or phases [13]. When all of these procedures or phases are combined, a comprehensive penetration testing methodology emerges. While different approaches use different terminologies for various processes or phases, they all have the same goal. SP800 is a set of information security standards published by the National Institute of

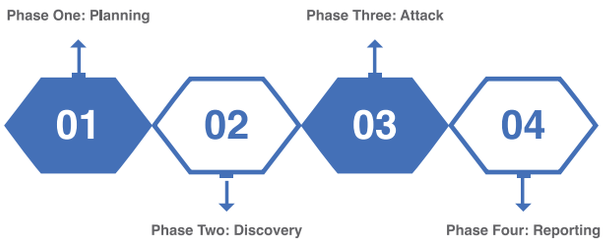


Fig. 2. Phases of Penetration Testing.

Standards and Technology (NIST) in the United States. Security testing approaches, system development life cycles, development strategies, and standard testing tools are all covered in SP800-42 [23].

Penetration testing employs the same tactics used by hackers to uncover flaws in a company's security system. This aids in identifying any aspects of the system that need to be evaluated in order to address reported flaws. The process of penetration testing can be separated into four stages [10], as shown in Fig. 2.

III. Methodology

A. Research Design

According to a recent study, small and medium enterprises (SMEs) have a significant representation within the global economy [6, 25]. Indeed, records show that businesses—and especially SMEs—have been increasingly relying on information technology and internet expansion. This has led to the emergence of different dangers to information security that can severely impact businesses should they be compromised [11].

The main objective of this study was to explore the role of automated penetration testing tools in small organizations to increase their security without hiring penetration testers. An ethical application document was submitted to the ethics committee of the College of Computing and information technology at the University of Shaqra to investigate and resolve any ethical issues regarding human rights violations and safeguard the privacy and anonymity of the participants (the IRB approval number:00105102022).

To determine whether or not automated penetration testing tools are practical for small businesses, the study needed to mimic a real case. For more reliable conclusions, it is important to model the real world as closely as possible in a case study. Therefore, the authors opted for a qualitative methodology to determine an organization's true state of cybersecurity. It is vital to determine the present degree of information security inside a business in order to evaluate the requirement for these penetration testing tools. Furthermore, examining the outcomes of a proposed solution's execution is the most effective way to determine its viability. Accordingly, the research design employed a case study method for gathering the data necessary for answering the research questions.

The authors took great care in the selection of the organization. Indeed, the authors ensured that it was well-established, able to handle a high volume of requests, was roughly an average size (based on revenue). It had fewer than 50 employees, and housed a dedicated technology division. The selected business would be the most representative of small businesses as a whole and their actual cybersecurity requirements.

Al Ber Charitable Society is the subject of the case study for this investigation. Established in 1982, the targeted society received approval from the Minister of Labor and Social Affairs in September 1985 [28] to formally register as the Al Ber Charitable in the Afif Governorate. Given the research purpose, the authors opted for the case study approach as identifying cybersecurity threats requires conducting penetrative tests on varying levels to assess the information security level of this SME. The method allows one to establish a realistic case scenario, which in turn allows for the generation of more trustworthy findings that reflect the applicability of these technologies in smaller enterprises with greater accuracy. To accomplish the study's goals, this research methodology was conducted in four phases: (1) Interviewing employees from the society, (2) analyzing the interview data, (3) conducting experimental testing of automated penetrating tools, and (4) interpreting the results. The results from the earlier stages were taken into account while designing subsequent stages. Fig. 3 illustrates how this research was conducted.

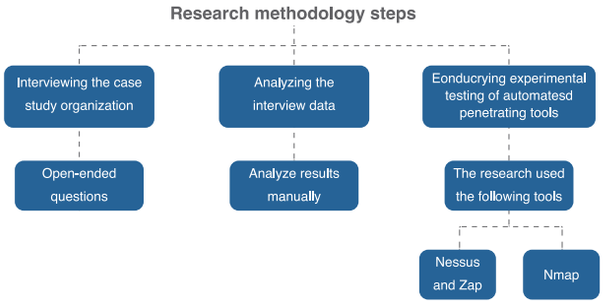


Fig. 3. The research methodology steps.

B. Data Collection

This study employed the case study approach for gathering data. This involved qualitative methods that included the use of a structured personal interview and experimentation methods. The former was used to determine the attitudes and overall awareness of the workers toward cybersecurity concerns. The structured interviews consisted of open-ended questions that were posed to six employees (who were responsible for specific organizational tasks) before the experimentation process. The authors selected those six participants as they had an initial understanding and knowledge of information security measures and how these would relate to penetration testing and cybersecurity.

Despite the advantages of the interview process, it is especially time-consuming in data collection and analysis. In addition, the lack of rapport between an interviewer and an interviewee can cause difficulties in the data collection as some individuals would be less likely to express themselves. Furthermore, the interviewer may be biased, which could affect the credibility and reliability of the research.

Additionally, the authors used the observation method to collect data on employee attitudes and behaviors regarding information security. Monitoring employee activities has been chosen as one of the fundamental measures for cybersecurity in companies and organizations. According to previous research, monitoring employee activities can help detect cyber-attacks and threats early, as well as reduce the risks of internal leaks, and data manipulation, and protect sensitive information. Additionally, monitoring employee activities can help to improve employee behavior and enhance the security culture within the organization, which helps to maintain the integrity of the systems and critical data of the company [16].

The authors considered this method essential as it would allow for an accurate analysis of employee perceptions and countermeasures during the interview with the six employees.

C. Automated penetration testing tools

A penetration test, colloquially known as a pen test, pentest, or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system [22].

Security Assessments

- Security Assessment – Test performed to assess a network or system's level of security.
- Security Audit – Policy and procedure focused; tests whether an organization is following specific standards and policies; searches for compliance only.
- Vulnerability Assessment – Scans and tests for vulnerabilities but does not intentionally exploit them.
- Penetration Test – Looks for vulnerabilities and actively seeks to exploit them [22].
- In the second phase of the study, the Security Assessment and Vulnerability Assessment were adopted in the penetration testing process on the Al Ber Charitable Society in Afif Governorate, using automated penetration tools. A wide array of tools for automated penetration testing are available in the market for businesses of all sizes, including Metasploit, Immunity Canvas, Core Impact, and Pen Test Pro. The Research used the following tools:
  - NESSUS Tool.
  - OWASP ZAP Tool (ZEDD ATTACK PROXY Tool).
  - NMAP Tool.

These testing tools were preferred due to their being open-source software and easily accessible. Other desirable software, such as Acunetux was not considered due to the unavailability of the licensed versions. Thus, the authors used readily-available software to determine the effectiveness of automated penetration testing tools in evaluating the secu-

rity of the target organization. Using the software for a real-life case scenario experimentation allows for determining the cybersecurity concerns of an organization's application. This facilitates a more comprehensive investigation into the level of the security countermeasures taken and allows one to suggest appropriate recommendations for improving network security.

IV. Results and Discussion

A. Interview Outcomes

Research interviews are the first step used to gather information in this study. When asked if they had a department that carried out penetration testing and, if not, how they accomplished it, the manager's comments suggested that the company was aware of the necessity to do penetration testing and protect the security of its information. For instance, one of the managers responded as follows:

"Unfortunately, our company lacks a dedicated penetration testing team. We are equipped with a team of technical support experts that can help with any issues. With the assistance of an expert, and at some expense, the online and network vulnerabilities were investigated once."

It is clear from the response that the organization recognizes the issue, but it is possible that the high cost of bringing in an expert has dampened enthusiasm for implementing the necessary changes. Moreover, the respondent mentioned that they would rather have someone on staff who can do the tests than hire an outside expert.

According to their comments, although the company was established thirty years ago, there has never been a report of a breach of information security occurring within it. The company has invested heavily over the past few years to fix its cybersecurity issues which were caused by employees acting based on their understanding rather than a codified information security strategy. This observation revealed that cybersecurity was a hot subject among the 35 employees and they all understood its significance. To sum up, small organizations should understand the need for penetration testing. However, the majority of people would opt not to undertake things because of their limited financial resources. Accordingly, these comments pointed to the need for affordable, straightforward, and productive automated penetration testing that can be performed by web development teams in these firms [16].

B. Results Concerning Web Penetration Testing Tools

As part of the experimentation process, the society's website (https://afifalbr.org.sa) was subjected to various tests to determine vulnerabilities in its system. The authors employed the Nessus and ZAP automated penetration tools to determine the vulnerabilities within the website application.

1) Nessus

The vulnerability checks are handled through plug-ins, which are distinct files. This simplifies the process of installing plug-ins and checking which ones are active so as to ensure that you are up to date. Nessus uses the server-client architecture. The advantages are that one can quickly and correctly identify vulnerabilities, configuration issues, and malware in physical, virtual, and cloud environments using Nessus scan services. [18, 26].

In Fig. 4, the results from the Nessus penetration testing tool indicate that the organization's website had one low-risk vulnerability while the rest of the other vulnerabilities are informational risks. This shows that the system had a moderate level of security that would not lead to any major threats, according to the results. While Fig. 5 below shows that the system did not have any major vulnerabilities that would have led to immediate measures against high-risk threats, Fig. 6 indicates that the low-risk threat detected was a POP3 Clear text login permission that hackers could easily exploit to gain access.

From the website's automated penetration testing, it was determined that the website had various vulnerabilities that impacted it. According to Nessus, there were 37 counts of vulnerabilities discovered on the web application. The highest risk was one low-risk vulnerability that had a test score of 2.6, which indicated that the remote host was running a POP3 Daemon. Daemon allowed for cleared logins over an encrypted connection that could allow cyber-attacks to gain access to user names

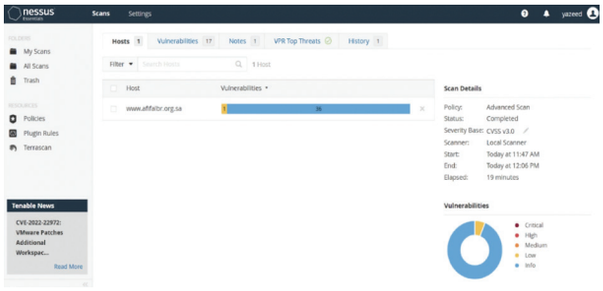


Fig. 4. Host Website Test Results.

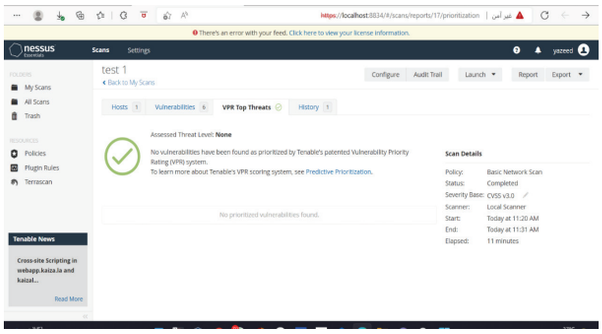


Fig. 5. Nessus Vulnerabilities Detected on Host Site.

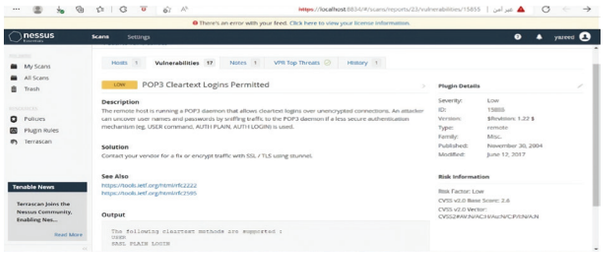


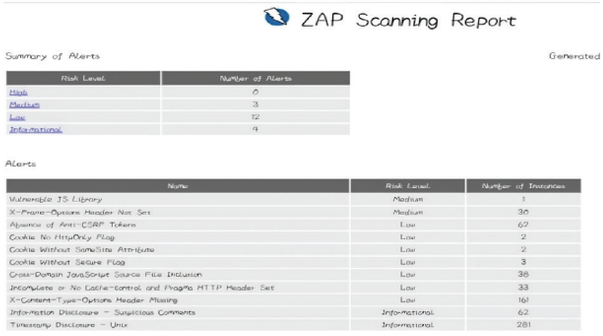
Fig. 6. Low-Risk Threat Detected.

and passwords by simply sniffing the traffic. The other vulnerabilities discovered were informational vulnerabilities that possess little to no risk to the system and did not disseminate sensitive information. However, the system was noted to have various open channels which exposed it.

2) ZAP

ZAP includes a variety of scan modes that can be used for various purposes. It generates a list of the vulnerabilities discovered during the scan. The Alerts tab, which is positioned in the bottom pane, displays these issues. Cooler-coded flags, red, orange, yellow, and blue, are used to identify all the vulnerability risk levels from high, medium, low, and no risk concerns, respectively. The "Report" menu option at the top of the screen can also be used to generate an HTML scan report. Fig. 7 shows the results of the test that was conducted.

The ZAP automated penetration testing program revealed that there were a large number of flaws in the online application. There were three moderate, twelve minor, and four informational risks in the system. The use of a vulnerable JS library and the failure to send the proper frame parameters caused medium-level warnings. If an attacker manages to get a system's login credentials, then sensitive data may be exposed and the system may be vulnerable to attack. Moreover, it was discovered that the HTML submission forms did not generate any Anti-CSRF tokens and that cookies were placed without the HTTP-only setting. As a result of these cookies being set without the proper security flags, being accessible by JavaScript, and not having the necessary SameSite characteristics, the system became more susceptible to cross-site request forgery and timing attacks. The ZAP tool revealed that the website was vulnerable to sniffers and lacked a cache-control header. The penetration tool indicated that there were a number of security issues with the website's application, which must be addressed. To do this, it is necessary to update the website to the newest version of Bootstrap and check that the cookies, cache-control header, and Anti-CSRF tokens are all properly configured. Also, any comments that may provide information to the attacker should be deleted from the site.



ZAP Scanning Report

Summary of Alerts

Generated

Risk Level	Number of Alerts
High	0
Medium	3
Low	12
Informational	4

Alerts

Name	Risk Level	Number of Instances
Vulnerable JS Library	Medium	1
X-Frame-Options Header Not Set	Medium	30
Absence of Anti-CSRF Tokens	Low	67
Cookie No HttpOnly Flag	Low	2
Cookie Without SameSite Attribute	Low	2
Cookie Without Secure Flag	Low	3
Cross-Domain JavaScript Source File Inclusion	Low	36
Incomplete or No Cache-control and Pragma HTTP Header Set	Low	33
X-Content-Type-Options Header Missing	Low	161
Information Disclosure - Suspicious Comments	Informational	62
Timestamp Disclosure - Unix	Informational	281

Fig. 7. ZAP Scanning Report on Al Ber Charitable Website.

C. Network Penetration Testing Tools and Results

Network Mapper, commonly known as NMAP, is a free and open-source instrument for preliminary scanning of systems or networks. This tool is typically employed during the initial stage of penetration testing due to its practical features. Some of the most valuable NMAP functions include gaining an understanding of a specific network, identifying available hosts within the network, determining the operating systems in use, and discovering ports. NMAP is suitable for scanning networks of various sizes [23]. The assessment was conducted using NMAP and the Nessus tool, targeting the host IP address (192.168.1.18).

1) NMAP and Nessus

This tool is consistently employed during the initial stage of penetration testing due to its practical features. NMAP's most valuable utilities involve understanding a specific network, such as identifying available hosts, determining the operating systems in use, and discovering ports. Moreover, NMAP is appropriate for scanning networks of various sizes.

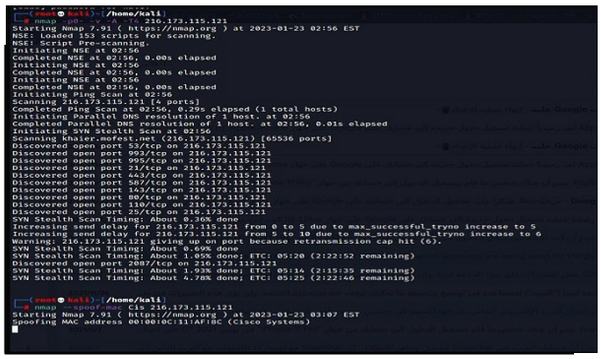


Fig. 8. NMAP Testing Results.

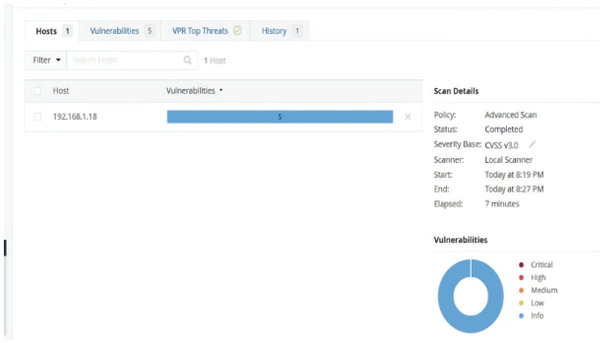


Fig. 9. Nessus Testing Results.

Fig. 8 and Fig. 9 show the results of the test that was conducted.

The automated penetration tool was used to scan a total of 65535 ports. From the results, it was discovered that, there were many open ports that hackers could manipulate to access the system, especially File Transfer Protocols and the Microsoft terminal service. Twenty-one TCP posts designated for the FTP were found open.

D. Discussion

The results revealed that automated penetration testing could be carried out in small organizations, especially by employing the ZAP, Nessus, and NMAP tools. Each of these three tools is readily available, open-source that would not lead to any extra costs incurred in purchasing licenses. In addition, the software allows cross-platform operating systems to be used on both Linux and Windows, making it easier to ensure compatibility. The tools are also quite easy to use; thus, they do not require professional help to analyze the vulnerabilities of the website and the network.

Therefore, automated penetration testing can be performed in small organizations using open-source software by following the detailed procedures outlined while explaining the various common testing tools.

Table II and Fig. 10 compare the risks evaluated by the Nessus, Zap, and Nmap tools for the website application and network.

In addition, through the experimentation of the three tools, it is noted that several ports were found open in all the analyses that would lead to exposure of the system to vulnerabilities should an attacker make use of these channels to access their information as the encryption was also found to be lacking. Table III shows the number of ports that were found open by the automated penetrative tools testing.

Fig. 11 shows the comparison between the Nessus tool and Nmap in terms of scanning the network outlets.

A significant gap emerged between the risk evaluation capabilities of the various tools. Fig. 8 shows that while the NESSUS tool was able to discover just one low-risk vulnerability, the Zap tool was able to identify and notify the user of additional risks, particularly on the low and medium risks associated with inadequate cookie settings and a susceptible JS library. On the other side, NMAP demonstrated several security flaws by scanning for open ports. Using ZAP and NMAP to assess the security of a company's website and network can protect the company's information at a low cost. The Nessus tool simply signals a single low-risk warning that provides next to no information on the condition of the website; this would allow for a more complete analysis that examines the particular faults and their solutions inside the online application.

While this is true, it should be taken into account the value of the three open port systems. Countless TCP and other open ports can be discovered with the use of NMAP's SYN and UDP scan options. Nessus analyzes the system for any open TCP ports that may leave it susceptible, and if any are found, it recommends installing an IP filter to close them off from the Internet. Unfortunately, the number of ports inside the system is not provided by the Zap tool, despite the fact that it is quite effective at identifying the hazards involved and providing thorough remedies. NMAP is better than Nessus because it can complete the scan in much less time. To conduct a more credible and accurate examination of the system's credibility, automated testing will require the use of several software combinations.

Moreover, it is evident from these resources that each is cost-effective, especially considering that they are easily accessible at no additional expense. As an added advantage, these tools may be used by any business without the need for additional staff training or experience. Therefore, it would be more efficient and cost-effective than the manual penetration testing methods that need the services of a skilled professional.

TABLE II
Penetration Testing Methods and Results Yielded.

Type of Risk	Detected by Nessus	Detected by Zap	Detected by N-map
High risk	0	0	0
Medium risk	0	3	1
Low risk	1	12	1
Informational risk	16	4	21
Total	17	19	23

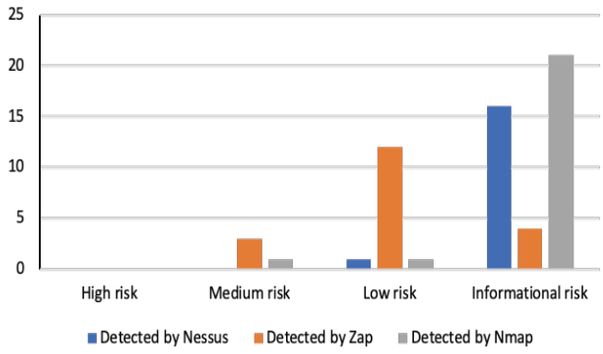


Fig. 10. Comparison of Vulnerabilities Detected by Web Automated Penetration Tools.

TABLE III
The Number of Open Ports Detected by Automated Penetration Tools.

Tool	Number of open ports scanned
Zap Automated Scan	0
Nessus Automated Scan	19
NMAP Automated Scan	23

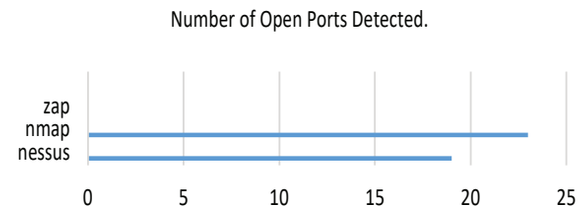


Fig. 11. The Number of Open Ports Detected in Nessus and Nmap.

V. Conclusion and Recommendations

A. Conclusion

The study investigated the efficiency of automated penetration testing for helping small businesses guarantee the safety of their customers' and users' data by vetting their websites and networks for vulnerabilities. According to the findings of the investigation, the case study of the nonprofit organization demonstrated that the organization was susceptible to cyberattacks, particularly those that are carried out by sniffing or social engineering. Taken together, all these vulnerabilities provide a far greater threat if they are exploited. According to the results, the company should implement the measures suggested by the testing tools in order to improve its cybersecurity. These included paying closer attention to the framework and cookies of the website, as well as using an IP filter to prevent attackers from making use of the open TCP channels available for file transfer protocols. This research demonstrated the viability of cross-platform automated penetration testing for small businesses by employing open-source software tools. This means that the tests may be conducted in companies of comparable size. The results indicated that penetration testing might be executed using a combination of technologies that would secure the data on open ports and existing vulnerabilities.

Our findings indicate that ZAP and NMAP are the most beneficial tools for assessing website and network vulnerabilities respectively. The study's findings confirmed that the toolset would provide an investigation of the website's apps' protocols and architecture and an evaluation of the network's current state. Therefore, using many tools in tandem would be preferable. Nessus, on the other hand, would make it possible to do penetration testing on the web app that runs the website. In comparison to the ZAP tool, it would not provide precise or comprehensive findings.

The results of this research suggest that automated penetration testing may be successfully implemented even in very small enterprises. Thus, utilizing the previously mentioned approach and technologies, network and system administrators in small and medium-sized businesses should be able to undertake in-house penetration testing. Put differently, automated penetration testing solutions are a practical, efficient, and inexpensive option that should be seriously considered by small businesses. Small and medium-sized businesses may want to reconsider their approach to automated penetration testing given the critical relevance of information security to the global economy and industry.

B. Limitations

The research itself was exposed to various limitations, such as the restriction of the sample size to one organization. This may have introduced bias as the organization in question may not have accurately represented the circumstances of other SMEs. Consequently, the interviewees were not forthcoming with information that only allowed for an observatory analysis of the attitude of the employees towards the need for information security and the measures that have been put in place.

The study could also have used more software in its experimentation. However, due to the lack of licenses to allow access to the automated penetrating software, the research scope had to be narrowed to open-source products. Nevertheless, despite these limitations, the objective of the study was achieved.

C. Recommendations and Future Directions

During the research, it was noted that different penetration tools have different capabilities, allowing individuals to secure their information security. The use of automated penetration testing tools would allow individuals to heighten security without calling upon the help of experts. As such, it is recommended that:

The targeted organization should improve its network infrastructure and website applications to prevent future cyberattacks that may employ sniffing to access its network and gain sensitive information that could be used to threaten the organization and its end-users.

- Small organizations should consider using automated penetration testing tools because they are feasible, effective, and inexpensive solutions.

- Automated penetration testing tools should be used in multiple combinations as different tools have different capabilities that would allow users to have a broader perspective of their information security levels to probe both the website application and network infrastructure.
- Future research should be conducted into how highly automated penetration testing can perform more processes and actions, as well as identify a greater number of vulnerabilities. In so doing, a uniform technique could assign risks to distinct operations that would allow a better determination of the overall risks involved.

Given the vital importance of information security to business and economics, it is necessary for SMEs to reconsider performing (highly feasible) automated penetration testing as regularly as possible to ensure their information security and prevent malicious persons from attacking their systems.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] M. Prictor, M. A. Lewis, A. J. Newson, M. Haas, S. Baba, H. Kim, M. Kokado, J. Minari, F. Molnar-Gabor, B. Yamamoto, and J. Kaye, "Dynamic consent: an evaluation and reporting framework," *Journal of Empirical Research on Human Research Ethics*, vol. 15, no. 3, pp. 175-186, 2020.

[2] S. Nagpure and S. Kurkure, "Vulnerability assessment and penetration testing of web application," in 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-6.

[3] A. Singhal, T. Winograd, and K. Scarfone, "Guide to secure web services," NIST Special Publication, vol. 800, no. 95, pp. 4, 2007.

[4] S. Ohrimenco, G. Borta, and V. Cernei, "Estimation of the Key Segments of the Cyber Crime Economics," in 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2021, pp. 103-107.

[5] P. Bramwell, Hands-on Penetration Testing on Windows: Unleash Kali Linux, PowerShell, and Windows Debugging Tools for Security Testing and Analysis. Birmingham, UK: Packt Publishing Ltd., 2018.

[6] A. Khan and R. P. Neha, "Analysis of Penetration Testing and Vulnerability in Computer Networks," GRD Journals-Global Research and Development Journal for Engineering, vol. 1, no. 6, 2016.

[7] A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis, and C. Peersman, "Scoping the cyber security body of knowledge," IEEE Security & Privacy, vol. 16, no. 3, pp. 96-102, 2018.

[8] H. Aldawood and G. Skinner, "Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal," International Journal of Security (IJS), vol. 10, no. 1, 2019.

[9] F. Alharbi, M. Alsulami, A. Al-Solami, Y. Al-Otaibi, M. Al-Osimi, F. Al-Qanor, and K. Al-Otaibi, "The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia," Sensors, vol. 21, no. 20, pp. 6901, 2021.

[10] A. Hasan and D. Meva, "Web application safety by penetration testing," International Journal of Advanced Studies of Scientific Research, vol. 3, no. 9, 2018.

[11] M. Moore, "Penetration testing and metasploit," no. April, 2017.

[12] G. M. Roberts, "Automated Network Exploitation Utilizing Bayesian Decision Networks," 2021.

[13] K. Barik, A. Abirami, S. Das, K. Konar, and A. Banerjee, "Penetration Testing Analysis with Standardized Report Generation," in 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021), Bangalore, India, 2021, pp. 365-372.

[14] A. Cordella, L. Bononi, and F. Crinò, "Web application penetration testing: an analysis of a corporate application according to OWASP guidelines."

[15] M. Ahmad and S. B. Maynard, "User activity monitoring for insider threat detection: A review," Computers & Security, vol. 68, pp. 81-97, 2017.

[16] D. J. Webb, C. L. Green, and T. G. Brashear, "Development and validation of scales to measure attitudes influencing monetary donations to charitable organizations," Journal of the Academy of Marketing Science, vol. 28, no. 2, pp. 299-309, 2000.

[17] C. R. Kothari, Research methodology: Methods and techniques. New Delhi, India: New Age International,

2004.

[18] A. P. Be Namanya, A. Cullen, I. U. Awan, and J. P. Disso, "The world of malware: An overview," in IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, 2018.

[19] F. Bertone, F. Lubrano, and K. Goga, "Artificial Intelligence Techniques to Prevent Cyber Attacks on Smart Grids," Annals of Disaster Risk Sciences: ADRS, vol. 3, no. 1, pp. 0-0, 2020.

[20] O. Kitapci, Ö. Tosun, M. F. Tuna, and T. Turk, "The use of artificial neural networks (Ann) in forecasting housing prices in Ankara, Turkey," Journal of Marketing and Consumer Behaviour in Emerging Markets, vol. 1, no. 5, pp. 4-14, 2017.

[21] A. Cordella, L. Bononi, and F. Crinò, "Web application penetration testing: An analysis of a corporate application according to OWASP guidelines."

[22] R. K. Kumar, "Introduction All New CEH v11," Github, June 22, 2022. [Online]. Available: https://github.com/imrk51/CEH-v11-Study-Guide/blob/main/modules/14-Pentesting.md. [Accessed: Jan. 15, 2023].

[23] J. Metso, Penetration testing: Ethical hacking, 2019.

[24] E. F. Dazet, "ANEX: Automated network exploitation through penetration testing," 2016.

[25] K. C. Goh, "Toward automated penetration testing intelligently with reinforcement Learning," Doctoral dissertation, Dublin, National College of Ireland, 2021.

[26] A. Khan and R. P. Neha, "Analysis of penetration testing and vulnerability in computer networks."

[27] R. Tuli, "Analyzing Network performance parameters using Wireshark," arXiv preprint arXiv:2302.03267, 2023.

[28] A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso, "The world of malware: An overview," in IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, 2018.

[29] J. Collins, "Mastering tcpdump for cyber security beginners," LinkedIn, Dec. 29, 2023. [Online]. Available: https://www.linkedin.com/pulse/mastering-tcpdump-cyber-security-beginners-jesse-collins-ruhnc/.

[30] Stevenson, "14 Free Cybersecurity Tools for Startups," Drata, Nov. 18, 2022. [Online]. Available: https://drata.com/blog/free-cybersecurity-tools. [Accessed: Mar. 2, 2024].

[31] "8 Best Penetration Testing Tools," LinkedIn, Feb. 27, 2024. [Online]. Available: https://www.linkedin.com/pulse/8-best-penetration-testing-tools-guru99-ni3uf/?trk=article-ssr-frontend-pulse_more-articles_related-content-card.

[32] M. Stuart, "Penetration testing methodologies," Doctoral dissertation, Utica College, 2020.

[33] M. Rak, G. Salzillo, and D. Granata, "ESSecA: An automated expert system for threat modelling and penetration testing for IoT ecosystems," Computers and Electrical Engineering, vol. 99, pp. 107721, 2022.

[34] T. Yik Ern, C. Yan Shaw, and G. Jun Hao, "Penetration testing assignment," 2019.

[35] R. Messier, CEH v10 Certified Ethical Hacker Study Guide. Hoboken, NJ: John Wiley & Sons, 2019.