UNIVERSITY OF TURKU

Penetration Testing in Small and Medium-sized Enterprises

Cyber Security
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Bhuwan Chhetri

Supervisors:
Antti Hakkala (University of Turku)
Seppo Virtanen (University of Turku)

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Bhuwan Chhetri
Title: Penetration Testing in Small and Medium-Sized Enterprises
Number of pages: 56
Date: July 2025

ABSTRACT

This thesis explores the role of penetration testing in enhancing cybersecurity within Small and Medium Enterprises, a sector that is mostly constrained by limited resources but is increasingly targeted by cyber threats. The study reviews ethical hacking concepts and their accompanying issues and then dives into penetration testing. The key topics include types, processes, advantages, and drawbacks of pen testing, as well as its specific applications and challenges within SMEs.

The research methodology involves a systematic review of peer-reviewed literature assessing what threats SMEs face and how effective current cybersecurity measures have been. The study also extends its scope to mention open-source tools in connection with web penetration testing tools, network scanning utilities, password cracking software, and vulnerability assessment toolset and analysis-comparable based on the tools' relevance, efficiency, and cost-effectiveness for SMEs.

The thesis equally contains recommendations and best practices designed for SMEs as well as the establishment of importance for adopting a cybersecurity framework and strategy for risk mitigation. A summary and conditions of the study findings will then culminate in proposed directions for future research. This work seeks to provide actionable insights for moving towards improved cybersecurity defenses within SMEs, responding to a volatile landscape of threats.

Keywords: penetration testing, cybersecurity, cyber-threats, ethical hacking, vulnerability, cybersecurity frameworks, open source.

Table of contents

SMEs	Small and Medium-Sized Enterprises
EU	European Union
IOS	International Organization for Standardization
WAF	Web application firewalls
IPS	Intrusive Prevention Systems
CIA	Confidentiality, Integrity, and Availability
NDA	Nondisclosure Agreement
GDPR	General Data Protection Regulation
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standards
HIPAA	Health Insurance Portability and Accountability Act
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework
IEEE	Institute of Electrical and Electronics Engineers
AI	Artificial Intelligence
ICS	Industrial control systems
IoT	Internet of Things
FIM	File Integrity Monitoring
IDS	Intrusion detection systems
ML	Machine learning
DDOS	Distributed Denial of Service
IS	Information system
NIDS	Network Based Intrusion Detection System
HIDS	Host Based Intrusion Detection System
ZAP	Zed Attack Proxy
OWASP	Open Web Application Security Project
BeFF	The Browser Exploitation Framework
GPL	General Public License
GUI	Graphic User Interface
CMERP	Coordinated Malware Eradication and Remediation Platform
CSF	Cyber Security Frameworks
CIS	Centre for Internet Security

ENISA	European Union Agency for Cyber Security
GDPR	General Data Protection Regulation

1 Introduction

1.1 Background

In today's world security is a worldwide issue. Quality assurance is a method used for preventing the mistakes and defects throughout production and ensuring final products or services of the highest integrity. Penetration testing is the security testing used to identify all the vulnerabilities and risks that could be exploited by the attacker in web applications, networks, or software applications.

According to the IBM Cost of data breach report 2024, the average total cost of a data breach increased from $4.45 million in 2023 to $4.88 million in 2021 and shows that the cost of a data breach has increased by 10% since the pandemic [1]. Many challenges are faced by the enterprises and lead to being the number one victim in comparison to the size of the enterprises. There have been also massive changes in the business environment during and after the Covid 2019. SMEs are forced to adopt technologies, which were not needed before to survive and be competitive in the global market. SMEs differentiate from big companies in terms of their number of employees, turnover revenue, and balance sheet. Small and medium-sized enterprises (SMEs) are considered small, but they represent 99% of all businesses in the EU. SMEs play a vital role in the economic development of many countries by creating employment opportunities. EU commission gives a brief description for distinguishing SME company if it satisfies the following condition [2]: -

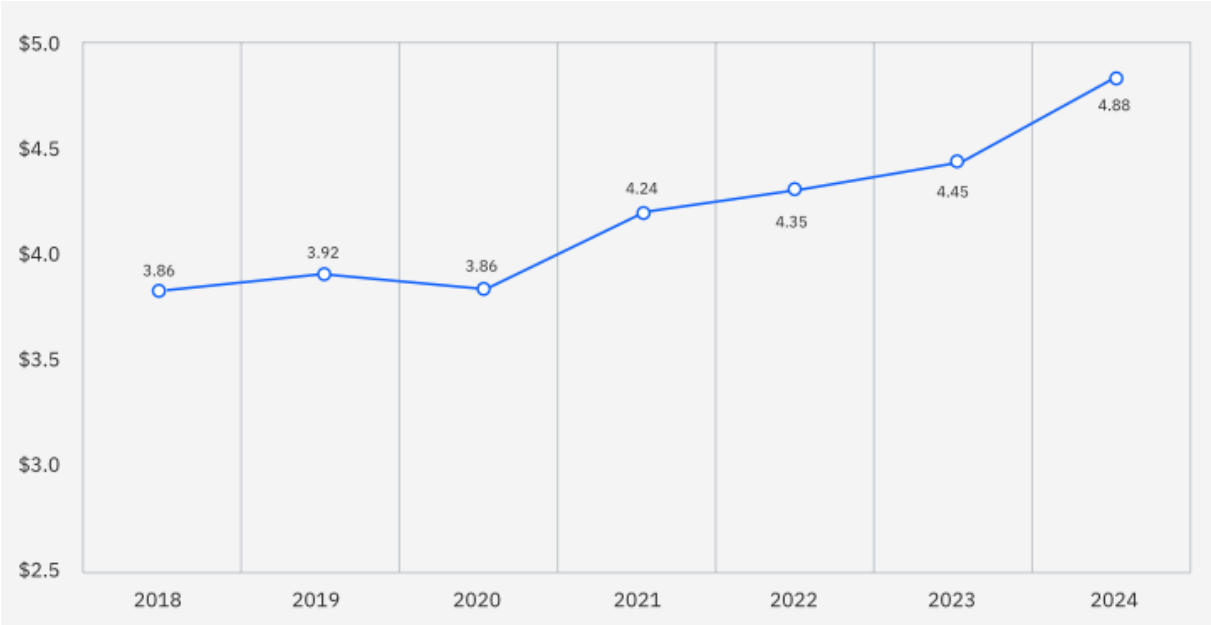
• < 250 and < 50 employees

• <= €50 m and <= € 10 m turnover

• <= €43 m and <= €10 m balance sheet total

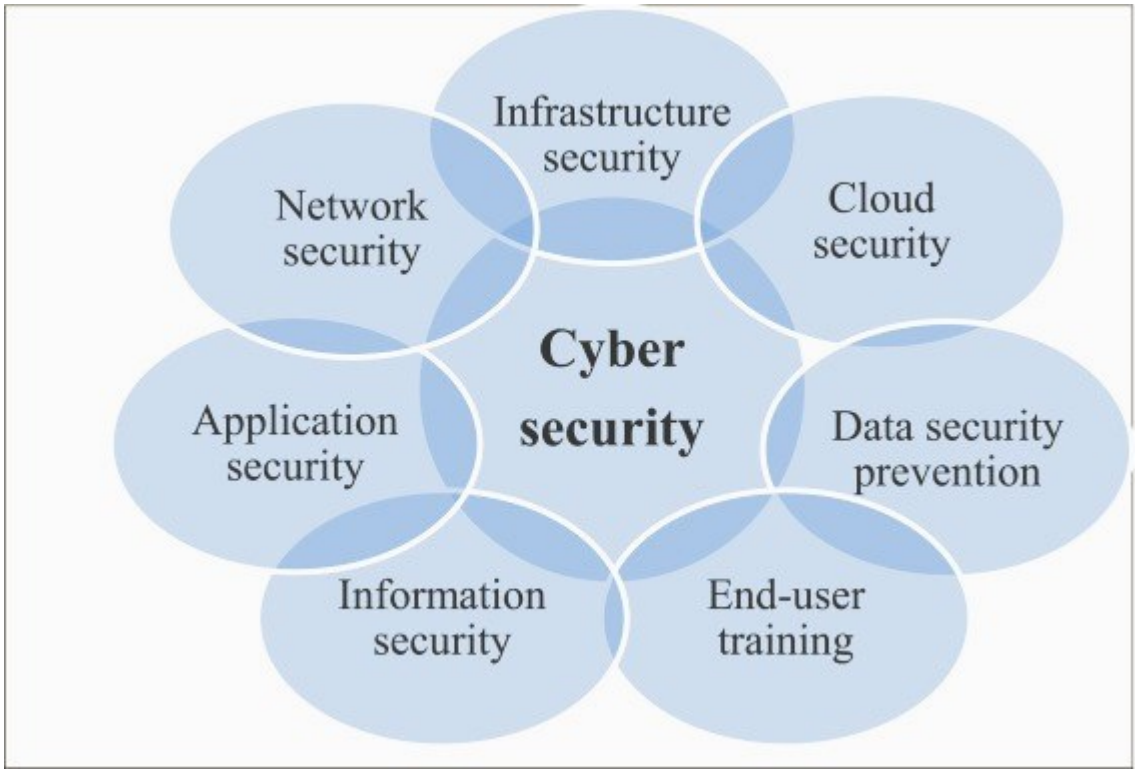
Every organization deploys security measures and certain frameworks to protect themselves against attackers. This alone does not give confidence about the success against the attackers. Penetration testing allows testing the strength of these security measures in real-time. Many tools are available for penetration testing and different stages of the process. If SME companies do not use penetration testing and certain frameworks, they will be more vulnerable and will eventually compromise their networks and confidential data, which can even cost their business. Figure 1 illustrates the global average cost of data breach measured in USD.

Figure 1 Global average total cost of data breach measured in USD millions [1]



Cyber-security is a well-known word in this era, as it has been an important issue in the foundation of every company and organization. By having intact cyber security most companies can achieve success and make their brand known as they will be successful in protecting the customer's data against their competitors. Every organization is competing to be on top in an unhealthy manner. Cyber security is a way to protect information, networks, and data against internal and external threats. There are different types of cyber security, so it is best to know the type of cyber security for better protection. Figure 2 illustrates the different types of cyber security.

Figure 2 Different Types of Cyber Security [3]



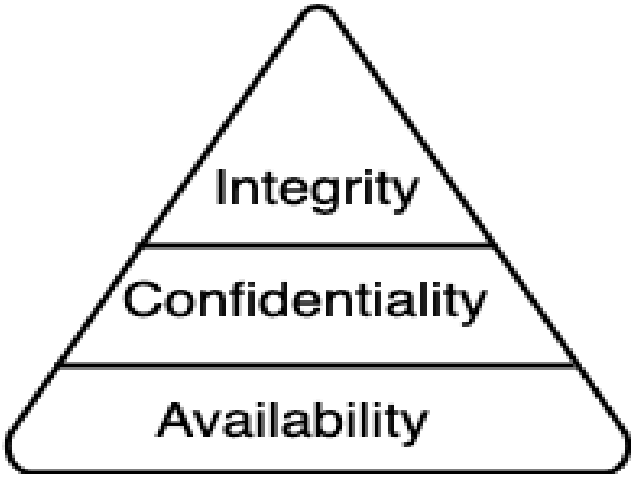
Network security - It protects the network inside the organization from organized attackers, hackers, and malware.

Application security - It protects software applications using hardware and software such as firewalls, web application firewalls (WAF), and intrusive prevention Systems (IPS).

Information security – It protects physical and digital data against any unauthorized access, disclosure, misuse, unauthorized changes, and deletion. The basic components of information security are known as the CIA triad: confidentiality, integrity, and availability [4]. Confidentiality means preventing unauthorized users and programs from accessing data. Information is frequently categorized according to its level of sensitivity, ranging the top secret and secret, which require the highest level of protection because disclosing them poses serious dangers to national security. There are unclassified data and not sensitive and are publicly available to anyone. Integrity means the data is kept accurate, concise, consistent, and has not been modified without authorization while being stored and transmitted. Availability means that information and devices are accessible to properly authorized users upon request.

Networked systems face threats to data availability from cyber-attack, equipment failures, or natural disasters. Figure 3 illustrates the CIA triad.

Figure 3 CIA Triad



End-user training – Educating the users on identifying and removing malicious attachments, refraining from connecting unauthorized USB devices, and addressing other significant security concerns ought to be integral components of any corporate security strategy [3].

Data Security – It is the practice of protecting digital information from unauthorized access, corruption, or theft through its entire lifecycle.

Cloud Security – It protects the information from internal and external threats in the cloud by following best practices, policies, and technologies.

Infrastructure Security – It involves protecting the tangible components that IT systems and networks rely on. This encompasses safeguarding the structures, server hardware, and additional physical assets from physical hazards, natural catastrophes, cyber-initiated attacks.

Cyber security professionals know the best way to protect the networks, servers, intranets, and computer systems. Cyber security ensures that only authorized person has access to the information.

1.2 Research questions

The research questions posed in this thesis are:
RQ1: How is SME security represented in penetration testing research from 2016-2025?

RQ2: What criteria should be used to evaluate open-source penetration testing tools for SMEs?
RQ2: What would be the ideal cybersecurity framework for SMEs to adopt?

1.3 Research methodology

This study employs a structured research methodology to explore penetration testing in SMEs, focusing on open-source tools. The methodology consists of a literature review, evaluation of tools in a controlled environment, and analysis of findings.

Literature Review:

A systematic literature review was conducted using various academic databases. The search strategy involved using specific keywords such as 'penetration testing', 'cybersecurity', 'information security' and 'SME' was used as most include filter. The searches were limited to publications from 2016 onwards to ensure relevance. The results were filtered based on their relevance to SME security challenges, penetration testing methodologies, and tool effectiveness. Duplicate articles, non-English and not accessible articles were removed. The following databases and search results were obtained:

Table 1 Topic selections

Database	Hits	Reviewed
Google Scholar	416	3
Scopus	60	1
IEEE Xplore	80	4
Web Science	19	1
Semantic Scholar	91	2

Using the keyword 'penetration testing' and sorting by the year 2016–2025, SME, information security, and cybersecurity in Google Scholar yielded about 416 results. Filtering the keyword penetration testing, SME, cybersecurity and information security within Computer Science in Scopus resulted in 60 hits. Searching for 'SME' and filtering with 'cybersecurity', SME, penetration testing and information security in IEEE Xplore returned 80 results. Using 'penetration testing, SME, information security and cybersecurity and year from 2016' in Web Science produced 19 results. Finally, searching for 'penetration testing,' 'SME,' 'cybersecurity,' and 'information security' in Semantic Scholar returned 91 results.

Evaluation of Open-Source Tools:

A selection of open-source penetration testing tools was tested in a controlled environment. The evaluation criteria included usability, effectiveness, scalability, cost, compatibility, automation, and community support. The tools were assessed using simulated attacks on test environments resembling SME infrastructure to determine their suitability.

Data Analysis:

The collected data from literature and tool testing were analyzed to identify trends, strengths, and weaknesses in SME cybersecurity practices. Comparisons between tools were made to recommend the most suitable options for SMEs based on their security needs and resource constraints.

1.4 Thesis structure

This thesis is structured into seven main chapters, each covering essential aspects of penetration testing in SMEs.

Chapter 1: Introduction – This chapter provides an overview of penetration testing, its importance for SMEs, and the research objectives. It includes the research questions and methodology used in the study.

Chapter 2: Penetration testing – This chapter explores penetration testing in detail, covering its definition, types, ethical considerations, and processes. It also discusses the advantages and drawbacks of penetration testing.

Chapter 3: Penetration testing in SMEs – This chapter examines the role of penetration testing in SME security. It highlights the benefits of penetration testing, the challenges SMEs face in implementing it, and the common cyber threats targeting SMEs.

Chapter 4: SME Security – This chapter focuses on the security landscape of SMEs. It discusses common security threats and challenges SMEs face, as well as the current security practices used to mitigate risks. Summary and the gaps from the literature review are analysed.

Chapter 5: Evaluation of Open-Source Penetration testing Tools for SMEs – This chapter presents an evaluation of open-source penetration testing tools based on predefined criteria. It includes an overview of different tools, their categorization, and an analysis of their effectiveness, usability, and suitability for SMEs.

Chapter 6: Recommendations and Best Practices for SMEs – This chapter provides cybersecurity frameworks and best practices for SMEs. It offers guidelines on improving security posture with limited resources.

Chapter 7: Conclusion – This chapter summarizes the key findings of the study, answers the research questions, and discusses future research directions.

2 Penetration testing

2.1 Overview

Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software, and people and can play a critical step in the development of any system or product [5] [6]. Penetration testing is the act of gaining access to networks or systems that resources without the knowledge of user credentials like usernames and passwords [7]. There are 3 different penetration-testing strategies, which are built on the amount of information available: -

a) Black box – The testers do not have any prior knowledge, and they figure out the loopholes of the systems it is like the real attacker who does not have any information related to the test target.
b) White box – The testers are provided with all the information related to the test target before the test.
c) Gray box – The testers are provided with partial information related to the test target and testers gather further information before the test.

2.2 Ethical Hacking

Ethical hacking is a procedure focused on securing the infrastructure and system [4]. Security experts break into the system and evaluate the targeted system without stealing the information and damaging the target, which is then reported back to the owner. Before diving into the penetration-testing domain, it is best to know about the ethical domain, as it is the backbone of the penetration-testing domain.

Numerous challenges surround the ethical domain. It is very important to underline the problem, verify the challenges, and solve them. These challenges are not limited to one but to various aspects. Some of the challenges in ethical domains are briefly mentioned below [5]: -

Capability challenges: Numerous challenges are related to the lack of skills and experience. Many ethical hacking teams have different skill sets, tools, and experiences compared to others when performing penetration tests.

Capacity challenges: Another challenge is performing penetration testing to analyze the security of enterprises against cyber-attacks regarding risk management [8]. The capacity is formed on the inexperienced manpower and available resources that are used to perform the penetration testing techniques and attack.

Cost challenges: The cost of conducting penetration testing is very high. penetration testing is divided into two steps, one step is to find out the existing vulnerabilities which is defined as cost, and the other is to fix the vulnerabilities and protect the system which is an additional cost.
Legal challenges: Many legal challenges surround ethical hackers and ethical hacking. penetration testing is not performed unless both the party ethical hacker and the organization that is conducting a penetration test sign a Nondisclosure Agreement (NDA).
Diverse challenges: These challenges depend on different ethical hacking groups; penetration testing technique, and their skills. Depending on the ethical hacking group, there is no certainty that vulnerabilities could be found by all groups. So, it is very hard and challenging to find the right penetration testing team to perform the task.
Knowledge challenges: This is the ability of ethical hackers to conduct penetration testing against security gaps and vulnerabilities.

2.2.1 Ethical Hacking Issues

Numerous issues surround the ethical hacking domain besides the challenge that we discussed earlier. Ethical hackers who lack skills, experience, and knowledge for a start have many different issues [9]. Some of the important issues are: -

a) Accuracy: The performed test and result may not always provide the right results as in reality; no system is 100% secure. Accuracy depends on the scenarios that penetration testing is conducted and to make sure that the system is secure from the attackers.
b) Accessibility: To conduct penetration testing, ethical hackers are given the least privileges to test the system, which might be an issue itself. Sometimes organization provides the least rights and privileges to ethical hackers to check their skill set due to the privacy policy of the organization.
c) Known attacks: In many cases, ethical hackers conduct penetration tests to evaluate company security measures against known threats. This is the reason that unknown attacks like zero-day attacks and polymorphic attacks are left behind.
d) Legal: Ethical hackers conduct penetration testing in real scenarios, and it is classified as cybercrime, which is why legal issues are highly emerging. So, it is important to sign the NDA to protect both sides. When performing such attacks everyone who can be affected should be informed.

e) Privacy: This is a very serious issue and should be taken seriously as ethical hackers perform penetration testing and perform simulated attacks. The target of the main attack of the simulation is confidentiality, integrity, and availability (CIA)

f) Security: These issues are related to the lack of skills, knowledge, and experience among the ethical hacking team, which is conducting a penetration test [10]. Many penetration testers lack or do not provide any security suggestions or recommendations.

g) Trust: It is one of the serious issues as ethical hackers have full inside knowledge of the organization, as they are involved in evaluating the security level of the company. The main concern would be finding the right black or grey hat hackers who are better trusted, and sensitive information could be in a safe place. That sensitive information could be leaked or sold to third parties without knowledge of the company which could damage and bring more serious issues.

h) Skill Gap: Skill gap is another issue, which is seen in penetration testers and ethical hackers. There has been a shortage or low availability of staff with the necessary security skills [11]. In the current situation, threats are becoming more advanced and sophisticated and security professionals are not able to deal with those threats and are not able to keep pace with the demand [11].

2.3 Types of Penetration Testing

There are mainly three areas, which define the scope and types of penetration testing: network penetration testing, application penetration testing, and social engineering.

a) Network penetration testing – Network penetration testing is the process of identifying security vulnerabilities in applications and systems by intentionally using various malicious techniques to evaluate the network security or lack of responses [12].

b) Application penetration testing – Application penetration testing is the process of performing diligent testing of applications to check for code-related or back-end vulnerabilities that provide access to the application itself, the underlying operating system, or the data that the application can access [13].

c) Social engineering – Social engineering is the process, which completely depends on human fault where sensitive and valuable data are gathered by using different methods, which also involves psychological manipulation.

2.4 Penetration Testing Process

There are systematic approaches that are used for penetration testing and the process needs to be well documented as they are presented to different organization units and management levels. There are 5 phases of penetration testing, which are briefly discussed below: -

a) Test preparation phase – The aim and the scope of the test are defined, agreed upon, and well documented. All the predicted incidents like downtime and information leakage are also identified and documented in legal documents and are agreed upon and signed by both parties

b) Information gathering – It is required to scan and identify all the physical and logical areas for the vulnerability analysis. Based on the collected information, the tester checks for vulnerabilities that could exist. This test can be automated, manual, or either.

c) Vulnerability analysis – The main aim of the vulnerability analysis is to identify and reduce the number of vulnerabilities before the software is deployed.

d) Vulnerability exploits – In this stage, the tester tries to exploit and gain access to the system by exploiting the vulnerabilities found during the vulnerability analysis session. Exploitation can have a big impact on the targeted system so exploitation should be performed if the client agrees to evaluate the impact of risks that can arise.

e) Test analysis – In this stage, the whole penetration testing process is compiled, and final reports are made and submitted to the management and technical staff. The report consists of various sections: Executive Summary, Test Scope, Results, Risk Level Indication, Recommendations, etc.

2.5 Penetration Testing Advantages and Disadvantages

Penetration testing has its advantages and disadvantages, which need to be understood before jumping into the penetration -testing environment which are explained in more detail below.

2.5.1 Penetration Testing Advantages

Penetration testing plays a critical role in the development of a secure product or system. Current business defines penetration testing as the application of automated network vulnerability scanners to an operational site, but true penetration testing is much more than that [6]. Penetration testing helps to find vulnerabilities and investigate data breaches and network intrusions. Many hacking tools are used by penetration testers to find already known faults and unknown vulnerabilities like software/hardware bugs, flows, and misconfigurations. It also tests the readiness of staff against the attack using social engineering and phishing attacks to evaluate the degree of readiness at the same time highlighting the security gaps. For small and medium-sized enterprises (SMEs), which are increasingly targeted by cyber threats, penetration testing offers several advantages that go beyond mere vulnerability identification.

a) Enhanced Security Posture

One of the primary advantages of penetration testing for SMEs is the improvement of their overall security posture. Penetration testing involves simulated cyberattacks that identify vulnerabilities in the organization's infrastructure. By addressing these vulnerabilities, SMEs can significantly reduce the risk of actual cyberattacks.

Identification of Weakness: Penetration testing provides a detailed assessment of security weaknesses in networks, applications, and systems. This information is crucial for SMEs, which often lack the resources for continuous security monitoring. The study conducted by Verizon highlights that vulnerabilities are the leading cause of data breaches, and it also emphasizes the importance of identifying and addressing them promptly [14].

Mitigation Strategies: The insights gained from penetration tests enable SMEs to implement targeted mitigation strategies, thus strengthening their defenses against potential attacks [15].

b) Cost-effectiveness

For SMEs, cost-effectiveness is a critical consideration in adopting cybersecurity measures. Penetration testing is a cost-effective solution that can save SMEs from significant financial losses associated with data breaches.

Preventing data breaches: The average cost of a data breach for SMEs can be devastating. Penetration testing helps prevent breaches by identifying and rectifying vulnerabilities before attackers can exploit them [15].

Optimized Security Spending: By pinpointing specific vulnerabilities, penetration testing allows SMEs to allocate their limited cyber security budgets more effectively, focusing on areas that need immediate attention [14].

c) Compliance and Regulatory Requirements

Many SMEs operate in industries that are subject to strict regulatory requirements. Penetration testing helps ensure compliance with these regulations, thereby avoiding legal penalties and enhancing customer trust.

Regulatory Compliance: Regular penetration tests are often mandated by industry standards and regulations such as GDPR, PCI DSS, and HIPAA. Compliance with these regulations not only avoids fines but also demonstrates a commitment to data security [16]

Building Customer Trust: Demonstrating robust security practices through regular penetration testing can enhance the trust of customers and partners, which is essential for business growth and reputation.

d) Risk Management

Penetration testing plays a crucial role in the broader context of risk management for SMEs. By understanding and mitigating risks, SMEs can ensure business continuity and resilience against cyber threats.

Risk Identification and Assessment: Penetration testing identifies risks that could impact business operations. This proactive approach aligned with principles outlined in NIST's Risk Management Framework (RMF) enables SMEs to assess the potential impact and likelihood of these risks. It provides a systematic approach to identifying vulnerabilities, assessing their impact, and ensuring accountability in the risk management process [17].

Business Continuity: By addressing vulnerabilities and planning for potential cyber incidents, penetration testing contributes to the development of effective incident response plans, ensuring business continuity [18].

e) Skill Development and Awareness

Conducting penetration tests also has the added advantage of enhancing the cybersecurity skills and awareness of SME staff.

Training and Awareness: The personnel of the organization are the most vulnerable elements in the execution of security measures, so to minimize the risk and ensure safety across the organization, security training is the most effective approach. Penetration testing exercises often include training sessions for IT staff, improving their ability to identify and

respond to security incidents. This enhances the overall security culture within the organization.

Skill Development: Regular penetration testing engagements provide opportunities for internal IT teams to learn from external experts, thereby building their own cyber security capabilities.

Penetration testing offers numerous advantages for SMEs, from enhancing security posture and ensuring compliance to cost-effectiveness and improved risk management. As cyber threats continue to evolve, the role of penetration testing becomes increasingly vital in safeguarding the assets and reputation of SMEs. By investing in regular penetration testing, SMEs can not only protect themselves against current threats but also build a resilient foundation for future growth.

2.5.2 Penetration Testing Disadvantages

While penetration testing provides significant advantages for SMEs, it also poses several challenges and potential drawbacks. This section explores the disadvantages of penetration testing for SMEs, drawing on contemporary research and case studies to offer a balanced perspective on this cyber security measure.

a) High Costs

One of the primary disadvantages of penetration testing for SMEs is the associated high costs [14].

Initial and Ongoing Expenses: Penetration testing can be expensive, particularly for small businesses with limited budgets. The costs include hiring external experts, acquiring tools, and potentially implementing recommended fixes.

Resource Allocation: The financial investment required for regular penetration testing may divert resources from other critical areas, such as general IT maintenance or employee training.

b) Disruption of Business Operations

Penetration testing can disrupt normal business operations, which can be particularly challenging for SMEs with limited operational flexibility [14].

Operational downtime: Conducting penetration tests often requires systems to be taken offline or operate in a reduced capacity, leading to downtime that can affect business continuity and productivity.

Interruption of Services: The testing process can inadvertently disrupt services, causing inconvenience to customers and potentially harming the SME's reputation.

c) Limited Scope and Effectiveness

The scope and effectiveness of penetration testing can be limited, especially for SMEs that may not afford comprehensive testing [14].

Incomplete Coverage: Budget constraints may force SMEs to limit the scope of penetration testing, resulting in certain systems or applications being inadequately tested.

False Sense of Security: SMEs might develop a false sense of security if the penetration test does not cover all potential vulnerabilities or emerging threats, leading to overlooked risks.

d) Dependency On External Expert

SMEs often rely on external experts to conduct penetration tests, which can introduce several issues [15].

Knowledge Transfer Issues: External testers may not fully understand the specific context and nuances of the SME's environment, potentially missing critical vulnerabilities unique to the organization.

Ongoing Dependence: Continuous reliance on external consultants for penetration testing can prevent SMEs from developing in-house cyber security capabilities, leading to long-term dependency.

e) Legal And Compliance Risk

There are legal and compliance risks associated with penetration testing, particularly if not conducted properly [16]

Unauthorized Access Issues: Improperly conducted penetration tests can lead to unauthorized access or data breaches, resulting in legal liabilities and reputational damage.

Regulatory Compliance: SMEs must ensure that penetration-testing activities comply with relevant regulations, which can be complex and resource-intensive to navigate.

While penetration testing is a crucial element of a cyber security strategy for SMEs, it does have its disadvantages. Significant considerations include high costs, potential business operation disruptions, limited scope, reliance on external experts, and legal risks. SMEs must

balance these drawbacks against the benefits to determine the most effective way to incorporate penetration testing into their cyber security practices.

3 Penetration Testing In SME

The penetration test for small and medium-sized enterprises (SMEs) offers insights for such companies. Every organization deploys security measures and certain frameworks to protect themselves against attackers. This alone does not give confidence to success against the attackers. Penetration testing allows testing the strength of these security measures in real -time. Many tools are available for penetration testing and different stages of the process. If SME companies do not use penetration testing and certain frameworks, they will be more vulnerable and will eventually compromise their networks and confidential data, which can even cost their business.

3.1 Benefits

a) Compliance – Penetration testing helps to stick to the various security regulations such as ISO 2700, PCI, and HIPAA. Avoiding the security regulations can result in the organizations receiving heavy fines, imprisonment, or ultimate failure [5].
b) Identifying the vulnerabilities – Business owners have false ideas about the hackers as they will not attack due to the size of the company. SMEs are the topmost target of hackers as vulnerabilities are easier to find. Penetration testing helps to find vulnerabilities that are not easily detected by the tools and software that are used inside the company.
c) Simulating real attack scenarios – Penetration testing provides much-needed experience to deal with the attacks that might arise in the future, without being invaded.
d) Prevent network downtime – When a business website is down due to security breaches or any other reasons there is a big loss for the company. Penetration testing ensures that there is zero downtime.
e) Awareness among the staff – Penetration testing ensures that all the staff are aware and following the security protocols. This is achieved using social engineering techniques.
f) Risk assessment – SMEs should have a good understanding of the information
g) Security and its importance in operating a business. Penetration testing can help businesses to know their weakness in technical infrastructure by providing a report with an extensive list of recommendations for the enterprises. These reports can be used to harden their system against malicious attackers [17].

3.2 Challenges

Small and medium-sized enterprises (SMEs) have globalization and digitalization challenges. They have very limited human and financial resources to adopt IT than the large companies and organizations. Due to the new way of working in recent years, it also has set completely new requirements for security strategies. The biggest inhibitors to defend against cyber threats in organizations are the lack of budget and low-security awareness among employees [18]. Security policy should be provided for employees today to work. As large data including personal information is also collected in SMEs, they should only be provided to the staff that need it for their work. There are always possibilities of unintentional human error from complex technology, which might lead to confidentiality and customer privacy data breaches. Attacks on complex systems require information about the target system; unfortunately, attackers are too often insiders, such as dissatisfied or reluctant employees. It is critical to improve the information security culture in organizations, the behaviors of employees should be following information security and related information processing policies and regulatory requirements [19].

3.3 Cyber Security Threats and Trends in SMEs

Being an easier target than larger companies, many risks lie to the SME. Helping SMEs to understand the main concept of cyber security can be a key solution and can be achieved by explaining the cyber security threats in SMEs. According to [20], small businesses saw an increase from $2.35 million in 2020 to $2.98 million in 2021, which is a 26.8% increase. Usually, SMEs underestimate cyber threats by not following efficient cyber security measures, which lead to a data breach, destruction of data, and refusal of access to data. The main reason for the SME's number one target is the weak defense mechanism used by the SMEs compared to the larger companies, less expertise, unknown outsourcing, and old security techniques. Training and education such as security policy and security awareness programs can play an important role in minimizing the threats as most cyber security attacks begin when the employee clicks on malicious links, emails etc. [21]. The survey conducted by Ipsos European Public Affairs shows the most dominant category of cybercriminal activity encompasses viruses, spyware, or malware, which have affected 14% of small and medium-sized enterprises (SMEs) within the preceding twelve months, followed closely by phishing, account takeover, or impersonation attacks, which impacted 11%. The remaining categories of cybercrime identified in the survey exhibit incidence rates (for the previous twelve months) of less than 5% [22].

Cybersecurity incidents have increasingly become a pressing issue for small and medium-sized enterprises (SMEs) throughout the Asia-Pacific (APAC) region. The survey conducted by ESET indicated that 70% of organizations faced a cybersecurity breach or detected significant indications of data security events in the past year, web-based attacks and data breaches were the most common incidents [23] . Specifically, India and New Zealand recorded the highest rates of incidents at 88%, followed by Japan at 73%, Malaysia at 70%, South Korea and Singapore both at 65%, and Australia at 60%. These results underscore the widespread and escalating influence of cyber threats on SMBs, highlighting the critical necessity for enhanced cybersecurity measures in the region. Figure 4 illustrates an overview of cyber security breaches occurring throughout the Asia-Pacific region and highlights common incidents [23].

Figure 4 Incident by country and most common incident [23]

4 SME Security

4.1 Common Security Practices in SMEs

Many techniques are used by many organizations, and many are custom-built. Custom-built applications and frameworks can cost thousands of euros and can be costly for SME businesses. Before diving into the custom built and frameworks that are used, 12 steps are introduced by the European Union Agency for Cyber security for SMEs [24] are discussed below which can help to minimize the attack and the treat SMEs possess:

1) Developing a good cyber security culture

Good practice of cyber security is the key element in the success of SMEs. Clear and specific rules should be defined in cyber security policies and should be abided, and policies should be regularly reviewed and updated. The auditors having skills, experience, and appropriate knowledge should carry out regular audits in the organization. EU general data protection regulation should be followed.

2) Providing appropriate training

Regular cyber security awareness training should be provided for all employees to ensure that they can recognize and deal with cyber threats.

3) Ensuring effective third-party management

The vendors who have access to sensitive information should meet all security requirements.

4) Developing an incident response plan

A formal incident plan should be made with clear guidelines, roles, and responsibilities to respond to the incident quickly. Tools should be used to monitor and create alerts for suspicious activity and security breaches.

5) Securing access to the system

Everyone should be encouraged to use a different character that consists of 12 characters long, numbers, upper-case and lower-case letters, and special characters. Multifactor authentication should be used for critical devices and infrastructure to prohibit unauthorized access.

6) Securing Devices

All the devices and software should be regularly updated and if possible centralized platform could be used for patching. VPN or SSL/TLS protocol should be used to access the website and file transferring outside the office network. If devices are reported stolen or lost, SME data should be wiped remotely.

7) Securing network

A firewall should be deployed to protect the SME network from the Internet. Remote access tools should be regularly reviewed to ensure they are secure and up to date.

8) Improving physical security

Physical controls should be employed wherever important information lies. All the devices and printed documents should not be left unattended, or an auto-lock function should be enabled on the devices.

9) Securing backups

Backup should be maintained, as they are very effective ways to recover from the cyber security breach

10) Engage with the cloud

Cloud solutions have many advantages, but laws and regulations should be followed to store the data.

11) Securing online site

Regular security tests should be carried out against websites to identify potential security weaknesses. All personal data or financial information should be protected.

12) Seeking and sharing information

Sharing information is one of the effective tools to fight against cybercrime. Cyber security challenges and solutions to those challenges should be shared among peers and industry; it will help to secure their system.

Over 60% of businesses use technical information security countermeasures such as antivirus software, firewalls, intrusion detection systems, anti-spyware software, virtual private networks (VPNs), vulnerability/patch management [25]. Some of them are explained below: -

a) Antivirus: The Antivirus system should always run the latest updates to be able to scan the latest virus signatures. It is very useful to eradicate malware from the system.

Sometimes it fails to detect the infected file if the file is encrypted or zipped. It should be noted that antiviruses are unable to detect zero-day malware.

b) Firewall: It is a network security device that monitors incoming and outgoing network traffic. It lets only those network packets transmit through it to the organizations, which fulfils the requirements that are set by the firewall administrator. Firewalls analyse the incoming traffic set by the firewall administrator and filters that are coming from suspicious and unsecured sources to prevent attacks. Firewalls can be software or hardware. A software firewall is installed on every computer and regulates traffic through applications and port numbers. A physical firewall is a device, which is installed between the network and the gateway.

c) Intrusion Detection System (IDS): IDS is one of the sets of computer security programs that detect threats or attacks before they are widely spread. There are two types of IDS systems, Network Based IDS (NIDS) and Host Based Intrusion Detection System (HIDS). NIDS is installed in a computer or device connected to the network and used to monitor network traffic. HIDS is installed on a computer or server, which is known as a host, and monitors only on that system. There are two categories of HIDS, signature-based and anomaly-based techniques [26].

4.2 Literature review on Cybersecurity in SMEs

The scientific research on SME cybersecurity highlights various factors contributing to their vulnerability to cyberattacks. Numerous studies indicate that small and medium-sized enterprises (SMEs) frequently overlook cybersecurity due to budget limitations, insufficient knowledge, and a lack of IT expertise. The investigation also examines prevalent threats, current security measures, and suggestions for enhancing the cybersecurity strategies of SMEs. Nonetheless, there is a scarcity of literature that specifically focuses on penetration testing in SMEs, highlighting a research gap regarding proactive security approaches for these enterprises.

To conduct a systematic review of relevant studies, a literature search was performed utilizing various academic databases. This research concentrated on cybersecurity threats faced by SMEs, their current security practices, and the significance of penetration testing in strengthening SME security. Table 2 presents a summary of crucial research articles chosen for consideration.

Table 2 A brief explanation of selected research

References	Year	Database	Summary
[27]	2023	Google Scholar	Attempts to develop an artificial intelligence framework aimed at identifying the cybersecurity needs of SMEs and delivering tailored security recommendations to assist them in managing cyber risks effectively.
[28]	2022	Google Scholar	Examines the determinants influencing the adoption of cybersecurity infrastructure in SMEs for the purpose of malware mitigation and proposes a conceptual framework to address these complexities.
[29]	2024	Google Scholar	Investigates the cybersecurity landscape within Small and Medium Enterprises (SMEs), revealing that despite their economic significance, SMEs encounter considerable cybersecurity challenges stemming from a lack of awareness, limited knowledge, and inadequate resources.
[30]	2021	IEEE	Introduces a cybersecurity assessment framework aimed at assisting SMEs in systematically identifying and addressing cybersecurity challenges within the context of Industry 4.0.

[31]	2023	IEEE	Conducts a comparative analysis of various security frameworks to ascertain the most appropriate one for SMEs, while considering parameters such as technical proficiency and financial implications.
[32]	2021	IEEE	Examines the issue of malware threats directed at SMEs and proposes a strategic framework to assist SMEs in addressing these threats effectively.
[18]	2016	IEEE	Underscores that the escalating digitalization of manufacturing heightens cyber security concerns, particularly for SMEs, who grapple with resource limitations and necessitate enhanced security measures to alleviate emerging cyber threats.
[33]	2023	Scopus	SMEs lack cyber security strategies and applying supervised machine learning methods in IDS can improve the network attacks in the system.
[34]	2024	Semantic	Explore the viability of open-source SIEM systems for SMEs by evaluating their security and performance capabilities.
[35]	2024	Semantic	Emphasizes the necessity of cybersecurity for SMEs, the risks they face, and the importance of aligning cybersecurity practices with frameworks like NIST and CSF.

[17]	2017	Web science	Summarizes the attack patterns and trends of various technologies, paying particular attention to the SME sector's cybersecurity obstacles.

The article “Unaware, unfunded and uneducated: A systematic Review of SME cybersecurity:” authored by C.Junior, I.Becker and S.Johnson [27], conducted a comprehensive systematic review of cybersecurity literature pertaining to small and medium-sized enterprises (SMEs) from the years 2017 to 2023. They meticulously examined the existing research regarding cyber threats, security measures, and the challenges that SMEs encounter in their endeavors to enhance their cybersecurity frameworks. Following an evaluation of 916 scholarly articles, they refined their selection to 77 pertinent papers and identified 44 predominant themes. The findings of the review elucidated that the body of research on SME cybersecurity is notably lacking in depth and has not significantly advanced the understanding of the specific cybersecurity requirements of SMEs. A considerable number of studies merely reiterate previously established findings rather than contributing novel insights to the field. Furthermore, the research highlights that SMEs face substantial challenges in cybersecurity due to insufficient awareness of risks, inadequate cybersecurity expertise, and limited financial resources to allocate towards cybersecurity measures. Additionally, these obstacles are observed to differ markedly between developed and developing nations. The authors posit that the lack of adequate cybersecurity knowledge is a principal factor contributing to SMEs' unawareness of risks and their insufficient allocation of resources.

The article “Cybersecurity Infrastructure adoption Model for Malware Mitigation in Small Medium Enterprises (SME) published in the IEEE 5th International Symposium in Robotics and Manufacturing Automation (ROMA), A.B.A. Ali, V.A. Ponnusamy, R.K. Ayyasamy, L.E. Heng, and R. Akbar [28] scrutinized the determinants that influence the implementation of cybersecurity infrastructure, categorizing them into technology, organization, and environment. The authors illuminated that malware represents a pivotal cybersecurity threat to the assets and operations of any organization. They further accentuated that SMEs are especially vulnerable to malware incursions due to their non-compliance with sufficient cybersecurity protocols. Additionally, Ali et al. observed a scarcity of research addressing the impediments associated

with the adoption of cybersecurity infrastructure for malware detection and mitigation, particularly within the context of Malaysian SMEs.

The article “A Cybersecurity Assessment Model for Small and Medium Enterprises” by A. Emer, M. Unterhofer, and E. Rauch, published in the IEEE Engineering Management Review (Vol.49, No.2) [30]examines the transformative shifts within the industrial landscape prompted by Industry 4.0 and the ensuing digital transformation. Small and Medium-sized Enterprises (SMEs) are increasingly adopting Industry 4.0 technologies to bolster their competitive edge. While Industry 4.0 avails advantages such as enhanced efficiency and flexibility, it simultaneously engenders new challenges, particularly a heightened vulnerability to cyber-attacks, a consequence of increased digitalization and connectivity. SMEs face distinct obstacles within this milieu, including elevated product complexity and the demand for mass customization. The integration of digital solutions for real-time data acquisition and dissemination is becoming indispensable for SMEs striving to maintain competitiveness. However, the digitalization journey poses significant challenges for SMEs, primarily due to a deficit in digital acumen. The importance of cybersecurity is magnifying for organizations undergoing digital transformations. SMEs necessitate cybersecurity solutions that are manageable, rapid, and offer sufficient protection against cyber threats, as they differ markedly from larger enterprises, which are the primary focus of cybersecurity technologies and service providers.

The article “Systematic Literature Review on Developing an AI Framework for SME Cybersecurity Identification and Personalised Recommendations” by H.M.T.N. Jayahilaka and J. Wijayanayake published in the Journal of Desk Research Review and Analysis, (Vol.2, Issue 1) [29] articulates that Small and Medium-sized Enterprises (SMEs) encounter cybersecurity challenges attributable to their limited resources and knowledge. Research indicates that SMEs frequently demonstrate a deficient appreciation of cyber risks, culminating in inadequate protective measures. Furthermore, SMEs encounter obstacles in the implementation of robust cybersecurity policies due to funding constraints, a lack of skilled personnel, and ignorance regarding potential threats. Although initiatives aimed at enhancing cybersecurity awareness and training for SMEs exist, these programs often lack the necessary specificity. The review accentuates the promising role of artificial intelligence in bolstering cybersecurity for SMEs by facilitating threat detection, risk evaluation, and mitigation strategies. However, extant AI-driven security solutions are predominantly constructed for larger organizations, thereby creating a void in the availability of tailored solutions suitable for resource-constrained SMEs.

The article “Comparison of Security Frameworks for SMEs” by G. Taskin, M.T. Sandikkaya [31], in International Conference on Electrical and Engineering (ELECO) conducts a comparative analysis of the IT audit of the Turkish Court of Accounts (TCA), the Information and Communication Security Guide (ICSG), ISO 27001, and NIST IR 7621. The objective of the study is to ascertain the most appropriate framework for SMEs, taking into account minimal technical expertise and financial constraints. Existing scholarly work predominantly concentrates on ISO 27001 and NIST IR 7621, while there is a notable paucity of focus on the IT audit of TCA and ICSG.

The article “Mitigating Malware Threats at Small Medium Enterprises (SME) Organization: A Review and Framework” by M. M. A. Mutalib, Z. Zainol, M. H. M. Halip [32] provides a detailed analysis of malware threats faced by SMEs and proposes a framework for mitigation. The authors effectively underscore the specific obstacles that SMEs face that limit their resources and technical expertise, which makes them a target for malware. The framework presented outlines technical, organizational, and procedural measures that constitute a holistic strategy for enhancing the resilience of SMEs against malware. One distinctive feature of the article, which is also one of its strengths, is that it provides a very specific target for SMEs, which are relatively underserved in cybersecurity-targeted studies. Further, the integration of theory and practice due to the gap analysis and the framework presented enhances the quality of the study.

The article “Security Challenges in Small-and Medium-Sized Manufacturing Enterprises” by M. Heikkila, A. Rattya, S. Pieska, and J. Jamsa [18], in the 2016 International Symposium on Small-Scale Intelligent Manufacturing Systems details the cybersecurity issues faced by the SME manufacturing industry. The authors present significant vulnerabilities that arise with the use of the interconnectivity of industrial control systems (ICS) and the implementation of IOT, which makes SMEs more susceptible to cyber threats. The authors argue that the lack of security standards poses a threat to lots of resources such as funds and other valuable resources that SMEs have at their disposal. The article highlights the risks posed by the digital transformation of a manufacturing firm; however, it overlooks a lot of practical analysis that is perfectly suited for SMEs. The article offers a useful perspective for understanding the unique cybersecurity challenges of SMEs in manufacturing and could serve as a foundation for further research in this sub-domain.

The article “The problem of information systems security in SME” by A. Alexei and A. Alexei [33], published in in the Central and Eastern European eDem and eGov Days 2023 (CEEeGov 2023), highlight that SMEs are attractive targets for cyber attackers due to their weak security measures compared to larger organizations, despite managing sensitive data. The authors' research indicates that the main issues faced by SMEs in ensuring information systems security include lack of budget, awareness, management support, effective security processes and tools, and employee awareness, with human error being a significant vulnerability. Furthermore, they emphasize that a study of security practices of SMEs in the USA shows that even when SMEs use anti-virus and firewall programs, they don’t update them, which is a critical oversight.

The article “Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs” by J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood [34], in "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," published in PLOS ONE, highlight that Small and Medium Enterprises (SMEs) are vulnerable to cyber threats due to inadequate protection, budgetary constraints, and lack of cybersecurity expertise. The authors also emphasize that while Security Information and Event Management (SIEM) systems are crucial for security monitoring, open-source SIEM systems have become prominent for their accessibility and cost-effectiveness. They further explain that their research evaluates the security and performance of open-source SIEM systems, addressing security challenges, regulatory compliance, resource utilization, and data processing in SME network environments.

The article “Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review” L. Ambreen, M. Jain, R. K. Yadav, and S. Loonkar [35] conducted a study on "Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review," which reviews the latest evaluations on the cybersecurity of SMEs, emphasizing the alignment of experiments with the NIST and Cyber Security Framework (CSF). The review discusses the importance of cybersecurity for SMEs in the digital age and the financial and reputational risks of cyber events. It also analyzes various cybersecurity risk management approaches, strategies, and frameworks and the study discovered that research in SME cyber security is sophisticated and specialized in attention on the NIST and CSF recognize as well as defend tasks, with minimal effort spent on the other current activities.

The article “A State of the Art Survey – Impact of Cyber Attacks on SME’s” by J. Saleem, B. Adebisi, R. Ande, and M. Hammoudeh [17], published in ACM International Conference Proceedings Series, Association for Computing Machinery, provides a critical exploration of the vulnerabilities faced by small and medium-sized enterprises (SMEs) in the context of cyberattacks. The study highlights the risks that small and medium enterprises (SMEs) encounter due to resource scarcity, insufficient technical personnel, and inadequate cybersecurity protocols. Finance, Business Operations, and reputation erosion, the result of such attacks are discussed, together with other issues, that SMEs have to face to restore their routine after these attacks. The most outstanding aspect of the article is the systematic filtering of the extant literature that brings forth information on major developments trends and developments in the cyber-attacks directed to SMEs. It is worth noting, however, that in as much as literature has provided secondary sources of information, the lack of empirical data case study has made the survey applicable only in theory. In summary, this article helps in recognizing the specific attributes of SMEs that need to be worked on in the quest for cyberspace security.

The reviewed literature demonstrates an increasing recognition of the cybersecurity challenges encountered by small and medium-sized enterprises (SMEs); however, numerous deficiencies and limitations remain evident. A principal concern is the absence of precise, actionable recommendations for SMEs regarding the implementation of cybersecurity strategies, particularly in the context of constrained resources. Although various studies routinely acknowledge the vulnerabilities inherent to SMEs alongside their resource limitations, they frequently fall short in providing comprehensive guidance on the effective utilization of available, cost-efficient resources, such as open-source penetration testing tools and cybersecurity frameworks.

In addition, literature elucidates discrepancies in the definitions and classifications of SMEs, which may impede the formulation of universally applicable cybersecurity solutions and frameworks. This ambiguity in standardized definitions complicates comparative analyses of research outcomes and the establishment of targeted strategic initiatives.

Furthermore, there exists a noticeable gap in empirical investigations that comprehensively assesses the practical application and efficacy of open-source penetration testing tools within the operational contexts of SMEs. Although the potential benefits of these tools are recognized, there is a scarcity of research pertaining to their integration into established cybersecurity frameworks to yield cost-effective and efficient security solutions for SMEs.

4.3 Threats and Challenges

With the advancement in technology, data security has become a major challenge for all-scale business organizations in securing communications channels, maintaining databases, and encryption techniques. Networks possess great risks and threats from attackers and any unprotected systems can be easily accessed to steal sensitive information. [36]. There are two major types of networking attacks, which are described below. [36].

a) Passive attacks - In these types of attacks, the attacker monitors or eavesdrops or monitors the data transmitted to find the content of data or analyzes traffic and decrypts weakly encrypted data and captures sensitive information. These types of attacks are hard to detect as no modification or alteration of data is done during the process.
b) Active attacks – In these types of attacks, the attacker tries to break into protected ongoing communication networks. These attacks are done by injecting malicious code or alteration of sensitive information. These types of attacks can be detected but they are hard to prevent. Some of the examples of active attacks are replay, denial of service, masquerading, and modification of message.

The most common cyber threats in SMEs are Phishing attacks, DDoS, Malware, Password attacks, Phishing Attacks, and spoofing. [37], which are briefly explained below.

a) Distributed Denial of Service (DDoS) - DDoS is a malicious attempt to interrupt the service or network by overwhelming the infrastructure with a flood of Internet traffic.
b) Malware – Malware is a term used to describe malicious software, including spyware, viruses, worms, and ransomware [38]. When users click a dangerous link or email attachment risky software is installed and the network and system are compromised without the knowledge of users. It is one of the great threats, which poses great risks to SME businesses as it can temporarily or permanently shut down the business [18].
c) Password Attacks – Password attacks are a term that involves cracking the user's passwords to gain unauthorized access to secure systems [37].
d) Phishing Attacks – It is a common cyber threat that is increasing every day. It is the practice of sending fraudulent communications that appear to come from reputable sources and it is usually sent in the form of an email [38]. The main goal of these attacks is to lure the victim to their replicate-designed website to steal sensitive information or to install malware on the victim's machine.

e) Spoofing – It is a cyber-attack that occurs when cybercriminals pretend to be legitimate companies and attempt to gain access to the system or steal important data and information.

Numerous challenges confront SMEs in safeguarding the organization, as emphasized by various researchers, which are outlined below: -

a) Low budget – They lack the proper budget to have ethical hackers and penetration testing to perform security flaws.

b) Lack of skilled employees – They lack skilled employees who are responsible for maintaining safety and security in an organization.

c) Negligence in security measures - SMEs are targeted more often than other big organizations because they often perceive cyber security as a waste of time and resources. Even when security fails or is attacked by the attackers, organizations do not take it seriously that they will be targeted the same year [18].

d) Lack of proper assessment tools (resources) - Proper assessment tools cost thousands of euros to perform the assessment.

e) Poor management – Employing employees in the wrong domain without having proper background checks which could have a serious impact on the organization.

f) Increase in use of IoT devices – Rapid growth of IoT devices, there are more risks in the exploitation of such technologies, and organizations are more prone to fall, victim.

g) Use of social media – Exposure to Internet space also brings a higher degree of threats and attacks [39]. SMEs are targeted by a wide variety of automated and non-automated attacks, which are followed by social engineering, and some of the attacks are derived from the misuse of the Information system (IS) in SMEs [39].

5 Selection Criteria of Open-Source Penetration Testing Tools for SMEs

In this section, we evaluate the effectiveness, usability, and relevance of open-source penetration testing tools for Small and Medium Enterprises (SMEs). Since SMEs often lack the resources to implement expensive proprietary cybersecurity solutions, open-source tools present a viable alternative. This evaluation examines the types of tools available, their advantages and limitations, and how well they meet the unique needs of SMEs.

5.1 Open – Source Tools

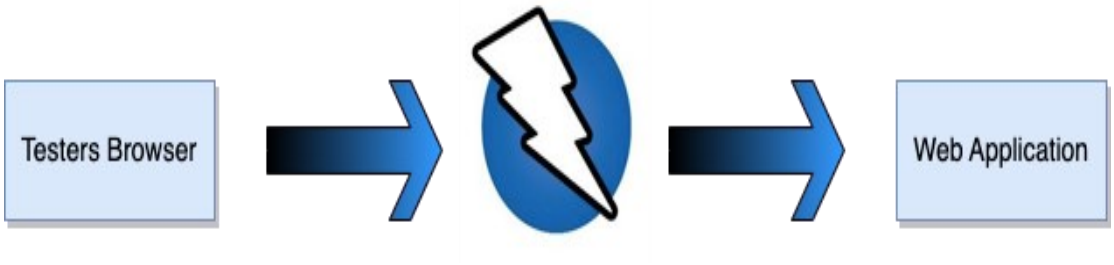
Many open-source tools are available and used in penetration testing. Many tools are freely available and used for different purposes. Some tools are used for web penetration testing; network testing, and password cracking, and some are for obtaining data that are not available for public viewing. Some of the popular open-source tools are briefly explained with their purpose, these tools can be very helpful for the SME business. Those tools were chosen because they are widely used, support comprehensive features, cross-platform availability.

5.1.1 Web Penetration Testing Tools

ZAP

ZAP is a free open-source penetration testing tool and is maintained under the umbrella of the OWASP [40]. OWASP stands for Open Web Application Security Project, which is a non-profit foundation that helps to improve the security of software. Zed is designed mainly for the testing of web applications and stands in between the tester's browser and web application. It is also known as a "man-in-the-middle proxy". It works in most of the OS systems and docker. Figure 5 illustrates the working mechanism of OWASP ZAP.

Figure 5 ZAP working [40]



Skipfish

Skipfish is a dynamic tool designed for web application security reconnaissance [41]. It creates an interactive sitemap of the target site by performing a recursive crawl and using dictionary-based probes. Skipfish is compatible with Windows, macOS, and Linux.

Wapiti

Wapiti is an open-source web application security scanner that helps identify vulnerabilities by performing black-box testing [42]. It scans web applications by injecting various payloads to detect security flaws such as SQL injection, XSS, and file inclusion. Wapiti is lightweight, easy to use, and supports multiple platforms, making it a valuable tool for security professionals and developers. Wapiti is compatible with Windows, macOS, and Linux.

Arachni

Arachni is an open-source web application security scanner designed to identify vulnerabilities in web applications [43]. It offers a modular and flexible framework, making it suitable for both individuals and enterprises. Arachni supports multiple platforms, including Windows, macOS, and Linux, and provides features like high-performance scanning, report generation, and integration with other security tools**.**

BeEF

BeEF stands for The Browser Exploitation Framework. BeEF is a penetration-testing tool, which is mainly focused on web browsers. It is designed to access the actual security posture of the targeted environment by using client-side attack vectors [44]. BeEF is compatible with Linux, Mac OS.

Burp Suite Community Edition

A free version of the popular Burp Suite tool provides essential features for web vulnerability scanning with some limitations in the free edition [45].

5.1.2 Network Scanning Tools

Nmap

Nmap is a free and open-source tool that is used to discover network and security auditing. It is widely used by penetration testers, networks, and system administrators. Nmap uses raw IP packets to determine the hosts available in the network, application name and version, running OS system, packet filters/firewalls that are used, and many other characteristics [46]. It is available in all major operating systems Linux, Windows, and Mac OS.

Netcat

Netcat is an old utility tool, which is known as the “Swiss Army Knife”. It is used for scanning the port and used in reading and writing data across the network connections, using the TCP/IP protocol [47]. It is available on Linux, SunOS/Solaris, and Mac OS.

Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform network scanner tool that is fast and simple to use. It scans IP addresses, ports, and other additional features such as NetBIOS info; favorite IP address ranges, web server detection, customizable openers, etc. [48]. It does not require any installations and is available for Linux, Windows, and Mac OS.

Legion

Legion is a fork of SECFORCE’s Sparta, which helps penetration testers in the scanning and enumeration phase [49]. Tools and commands are fully customizable with automation capabilities. It is recommended to use Kali Linux as most of the tools that are required to run Sparta are installed.

Metasploit

Metasploit is a powerful open-source penetration testing framework developed by Rapid7 for ethical hacking, vulnerability analysis, and exploit creation [50]. It supports various modules for payload scanning, payload generation, and maintaining access, making it a versatile tool for security assessments and penetration testing. It also includes auxiliary modules for network scanning, such as discovery and port scanning, enhancing its utility in network reconnaissance.

Masscan

Masscan is known as the ultra-fast network scanner designed for large-scale network discovery and reconnaissance [51]. It can transmit up to 10 million packets per second, making it capable of scanning the whole internet in under 5 minutes. Its output is like Nmap. It uses asynchronous transmission and a custom TCP/IP stack, enabling it to effectively scan and identify open ports across a large number of hosts.

5.1.3 Password Cracking Tools

John the Ripper

John the Ripper is an open-source tool used for security auditing and password recovery [52]. It is available for Unix flavors (Linux, Solaris, etc.), Mac OS, and Windows. There is also John the Ripper Pro that is available for commercial purposes.

Aircrack-ng

Aircrack-ng is a complete suite of tools to access Wi-Fi network security [53]. It can be used to crack the WPA and WEP passwords and for monitoring network traffic as well. It works on most of the OS systems like Windows, Mac OS, Linux, NetBSD, OpenBSD, Solaris, and eComStation2.

5.1.4 Vulnerability Assessment Tools

Nessus Essentials

Nessus takes the first place when it comes to the world of vulnerability assessment tools. In 2005 Nessus was changed from an open project to closed source and managed by

Tenable [54]. It is limited to 16 IPs per scanner in Nessus Essential. There is another commercial version Nessus Professional that comes with the price.

THC Hydra

THC Hydra is an open-source application that is used by penetration testers and security consultants to test security functionalities [55]. It supports one of the largest numbers of security protocols. It works on Windows, Mac OS, and Unix platforms. It is compatible with Linux, Windows, and Mac OS.

Open VAS

Open Vulnerability Assessment System (OpenVAS) is a full-featured vulnerability scanner [56]. It is developed and distributed by Greenbone Networks. It is provided with a high level of user configurability with a variety of built-in tests and web interface design. It is designed to run in a Linux environment and can be run either in a self-contained virtual machine or from source code provided under GNU General Public License (GPL).

Numerous open-source tools are available and can be used to detect intrusion, which is also a security goal for an organization. The security tools are briefly described below:-

SNORT

SNORT is a very powerful open-source Intrusion Prevention System (IPS). It is available in various Linux environments and Windows. It uses a series of rules that are defined as malicious, and it uses those rules to match against them and generates alerts for users [57]. It records the packets in human-readable form, and it is very easy to analyse and search.

OSSEC-HIDS

OSSEC is another powerful Host Based Intrusion Detection System (HIDS). OSSEC is mixed with integrating log analysis, file integrity monitoring (FIM), windows registry monitoring, rootkit detection, real-time alerting, centralized policy enforcement, and active response [58]. It is available in most of the operating systems like various Linux environments, MacOS, and Windows.

5.2 Analysis and Comparison of Tools

In this section, we will evaluate the tools based on criteria such as ease of use, effectiveness, flexibility, and community support, all of which are crucial in identifying the best tools for SMEs.

Some free, open-source web application scanner tools and network scanning tools are selected and compared to identify the best tools for specific needs which are illustrated in table 3 and 4.

Table 3 Comparison of different web application scanning tools

Features	**ZAP** [40]	**Skipfish** [41]	**Wapiti** [42]	**Arachni** [43]	**Burp Suite Community Edition** [45]	**BeEF**
Active Scanning	Yes	Yes	Yes	Yes	Limited	Yes
Passive Scanning	Yes	No	No	Yes	Yes	Yes
Fuzzing	Yes	No	No	No	No	Yes
Spidering/Crawling	Yes	Yes	Yes	Yes	No	No
Authentication Support	Yes	Yes	Yes	Yes	No	Yes
Report Generation	Yes (HTML, XML, JSON, etc.)	Yes (HTML, CSV, etc.)	Yes (HTML, XML, JSON, etc.)	Yes (HTML, XML, JSON, etc.)	No	Yes
Proxy support	Yes	Yes	Yes	Yes	Yes	Yes
SSL/TLS Support	Yes	Yes	Yes	Yes	Yes	Yes
Customizable Payloads	Yes	No	Yes	Yes	No	Yes
Ease of Use	User-friendly GUI	Command line interface	Command line interface	User-Friendly GUI	User-Friendly GUI	User-Friendly GUI

Community Support	Slack, GitHub	GitHub	GitHub	GitHub	PortSwigger	GitHub, Discord.
Community Add-ons	Yes	No	No	No	No	Yes
Release Date	2010	2012	2008	2010	2009	2006
Latest update	March 2025	January 2023	November 2024	May 2022	February 2025	November 2021
Cost	Free	Free	Free	Free	Free	Free
OS Support	Windows, macOS, Linux	Windows, macOS, Linux	WSL for Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Linux, macOS

Comparing the tools mentioned above, ZAP, Wapiti, and Burp Suite Community Edition stand out from the rest. Therefore, these three tools are selected for practical evaluation and will be analysed in the next section.

Table 4 Comparison of different Network scanning tools

Feature	Nmap [46]	Netcat [47]	Angry IP Scanner[48]	Legion [49]	Metasploit [50]	Masscan [51]
Port Scanning	Yes	Yes	Yes	Yes	Yes	Yes
Proxy Support	Yes	No	No	Yes	Yes	No
SSl/TLS Support	Yes	Yes	No	Yes	Yes	No
Customizable Payloads	yes	No	No	Yes	Yes	No
Ease Of Use	Command-line & GUI (Zenmap)	Command line interface	GUI	GUI	Command-line & GUI	Command-line & GUI
Cost	Free	Free	Free	Free	Free	Free

Community Support	GitHub, X, Reddit, Facebook	GitHub	GitHub	GitHub	GitHub, Slack, X. Mastodon	GitHub
Reporting & Documentation	Yes	No	Yes	Yes	Yes	Yes
Release date	1997	1995	2001	2018	2013	2001
Latest update	April 2024	March 1996	January 2025	February 2025	January 2025	January 2025
OS support	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux

Among the network scanning tools listed above, Nmap, Metasploit, Masscan, Angry IP Scanner, and Legion are the best choices due to their comprehensive features, ease of use, and strong community support. These tools are selected for the quick practical evaluation and will be analysed in the next section.

5.3 Practical Evaluation of open-source Tools

5.3.1 Web Application Scanner

In this section, an analysis of web application scanner tools is conducted, selecting only those mentioned in the previous section 5.1. This analysis was performed in my home lab. This lab was conducted by setting up DVWA vulnerable page.

In this chapter, shell commands are presented with the following style: [*sudo su*].

Step-by-step installation process is explained below.

Switching to Root User

Begin by switching to the root user to ensure you have the necessary permissions:

sudo su

Updating and Upgrading the System

Update and upgrade your Kali Linux machine to ensure all packages are current:

apt update && apt upgrade -y

Downloading DVWA

Download the DVWA zip file from GitHub, unzip it, and move the DVWA folder to the appropriate directory:

wget https://github.com/ethicalhack3r/DVWA/archive/master.zip

unzip master.zip

mv DVWA-master /opt/lampp/htdocs/DVWA

Starting XAMPP

Navigate to the XAMPP directory and start the XAMPP manager:

cd /opt/lampp

./manager-linux-x64.run

For downloading and installing XAMPP, visit Apache Friends.

Starting Services

Start the MySQL Database and Apache Web Server services from the XAMPP control panel.

Accessing XAMPP Dashboard

Once XAMPP is running, access the default dashboard page by navigating to http://localhost in your web browser.

Installing DVWA

Configure the DVWA page by editing the configuration file:

cd /opt/lampp/htdocs/DVWA/config

cp config.inc.php.dist config.inc.php

nano config.inc.php

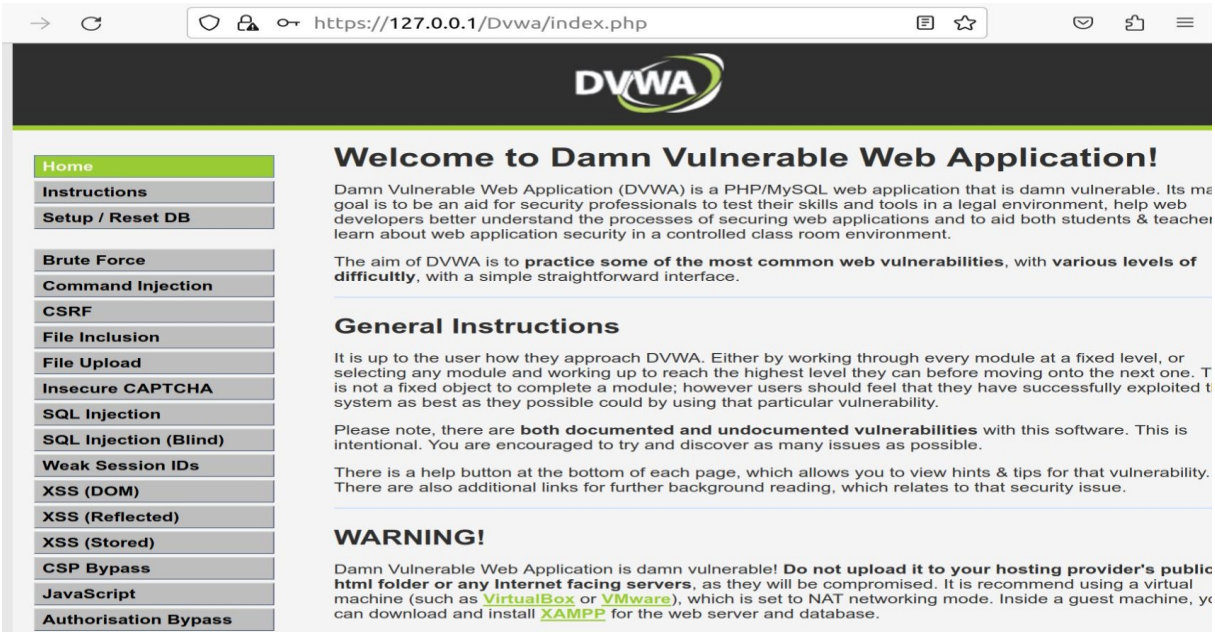
Set the appropriate username and password in the config.inc.php file.

Access DVWA

Navigate to http://127.0.0.1/DVWA in your web browser to access the DVWA page.

Figure 6 illustrates the welcome page of the Damn Vulnerable Web Application (DVWA), accessed via a web browser at https://127:0.0.1/Dvwa/index.php.

Figure 6 Starting DVWA page



ZAP

Install zaproxy

sudo apt install zaproxy

Scan the URL localhost/DVWA using an automated scan and AJAX spider with Firefox headless mode.

Figure 7 illustrates the automated scan tab in OWASP ZAP, where security scan is initiated by entering the target URL (http://127.0.0.1/Dvwa/index.php).

Figure 7 Automated Scan Interface in OWASP ZAP

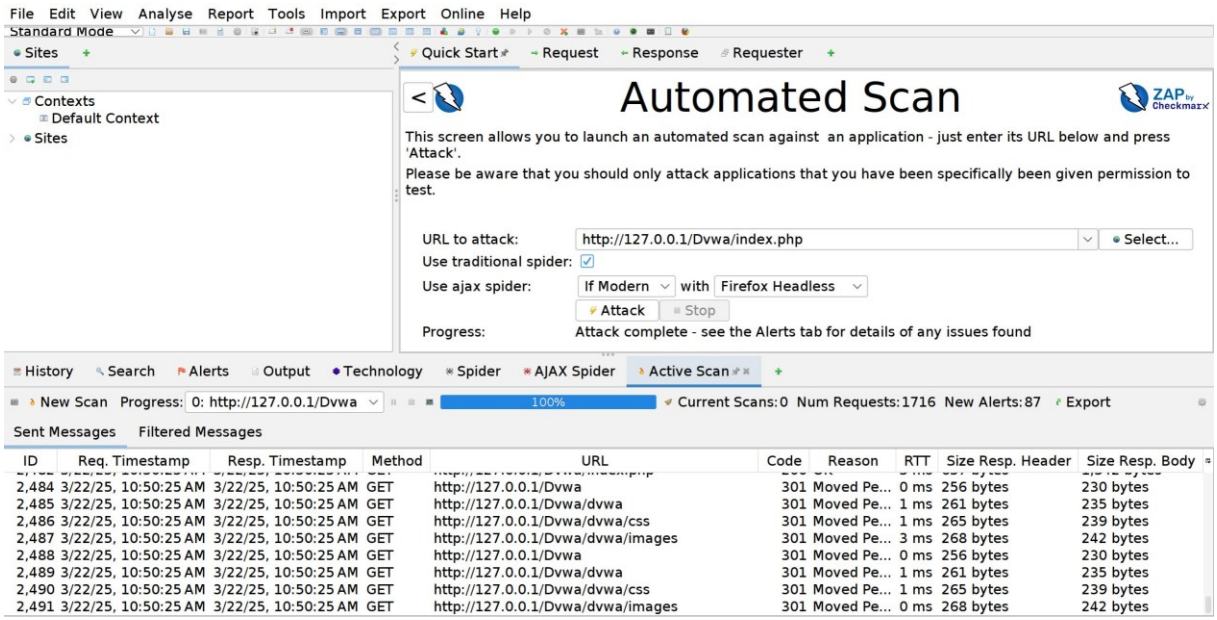
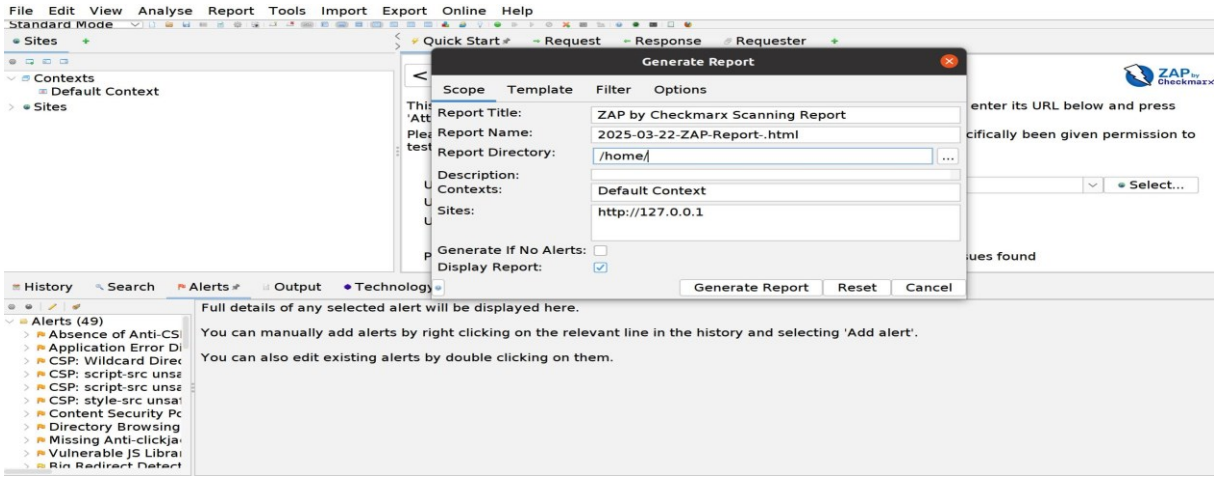


Figure 8 illustrates the process of generating and saving a scanning report in OWASP ZAP.

Figure 8 Saving Report



It is highly user-friendly and offers many useful features. The Alerts section provides detailed information on detected vulnerabilities and makes it easy to save the generated report.

WAPITI

Install wapiti

sudo apt install wapiti

for quick scan – *wapiti -u target_url*

Figure 9 illustrates a Wapiti scan targeting a web application located at http://127:0.0.1/Dvwa/index.php.

Figure 9 Wapiti scanning DVWA page

Start the DVWA page and perform a quick scan, which generates a report and saves it to a folder. Wapiti provides a wider range of options for selection during the scan.

Burp Suite Community Edition

Download the Burpsuite Community Edition from the PortSwigger website and choose the appropriate version.

Change file permission – *chmod +x burpsuite_community_linux_vX.X.X.sh*

Install Burpsuite Community Edition - *./burpsuite_community_linux_vX.X.X.sh*

Set up proxy – configure browser to use Burp Suite as a proxy or inbuilt proxy can be used. Set Burp suite to intercept web requests. Specify a target scope to filter out unwanted requests.

Open the DVWA page and perform a quick scan. Burp Suite Community provides a wider range of options for scanning and analysing web applications, including an intercepting proxy, request repeater, and basic vulnerability scanning.

Figure 10 illustrates a security testing scenario involving web application and web proxy tool, demonstrating a brute force attack.

Figure 10 Brute force with burp suite

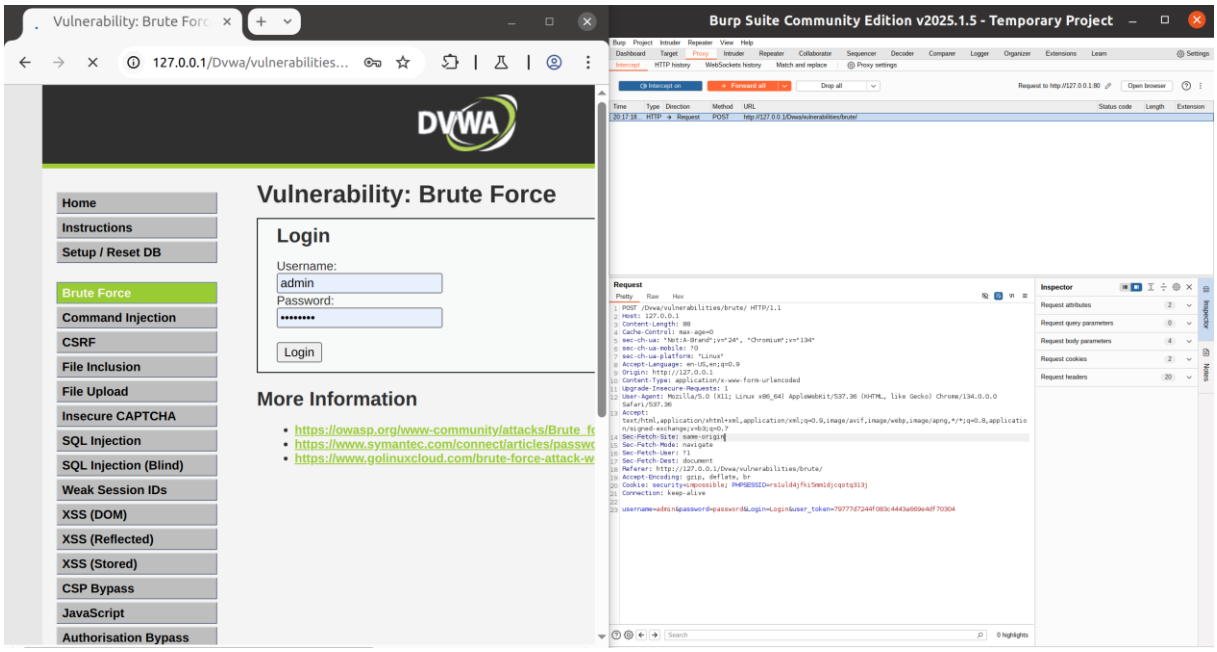


Figure 11 illustrates a security testing scenario involving web application and web proxy tool, demonstrating a SQL injection attack.

Figure 11 SQL injection with Burp suite

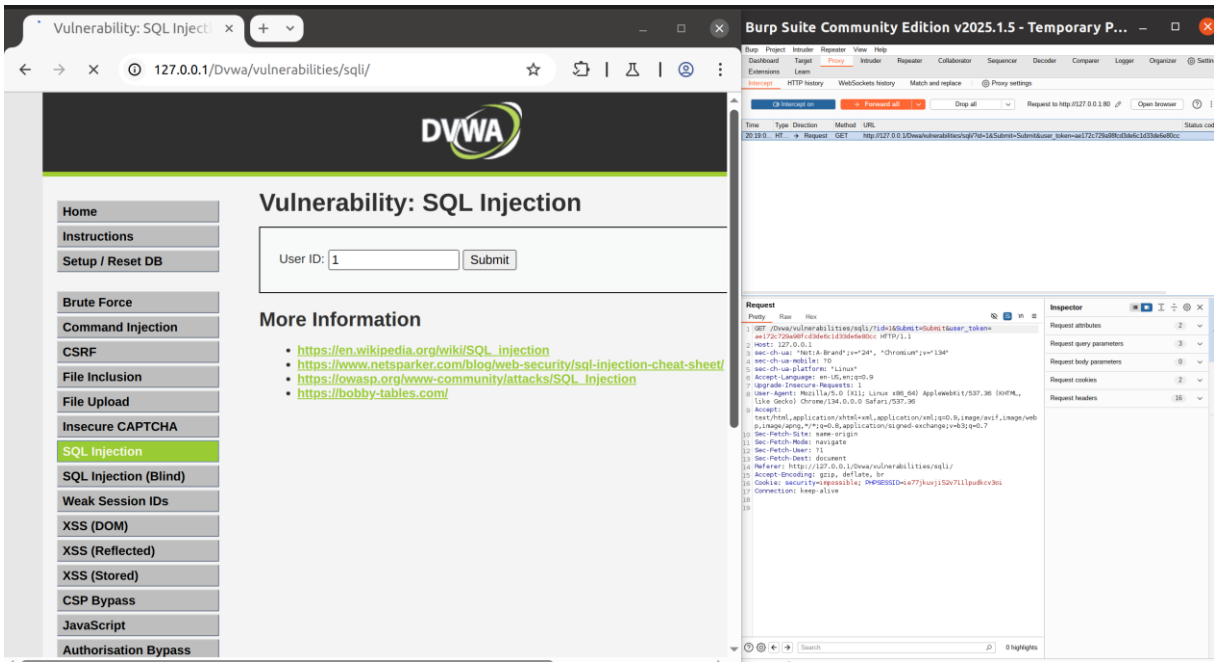
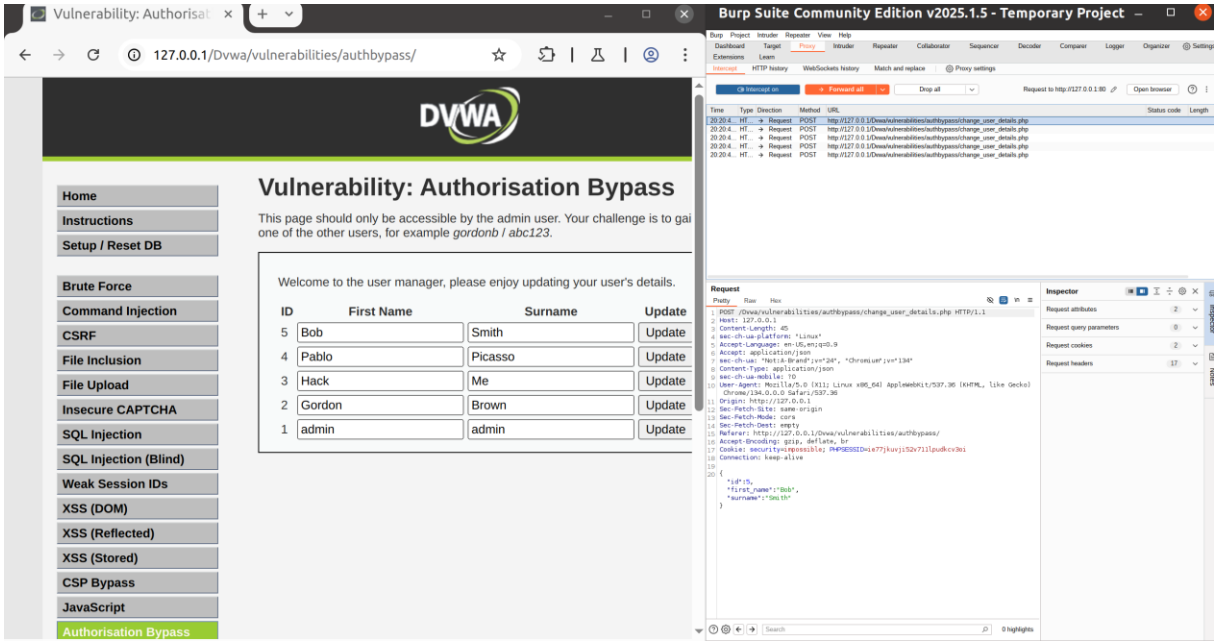


Figure 12 illustrates a security testing scenario involving we application and web proxy tool, demonstrating authorisation bypass attack.

Figure 12 Authorisation Bypass with Burp suite



Findings

From above analysis conducted ZAP seems to be the best, easy and highly user friendly. Burp suite comes with the many features and user need to have more expertise into it as it requires manual input.

5.3.2 Network Scanning Tools

In this section, an analysis of network scanning tools is conducted, selecting only those mentioned in the previous section 5.1. This analysis was performed in my home lab. This lab was conducted using Kali Linux installed in VMware.

Tools Used: Nmap, Legion, Angry IP Scanner

OS system: Windows 10

IP address: 192.168.101.106

Port Range: 1 – 1023

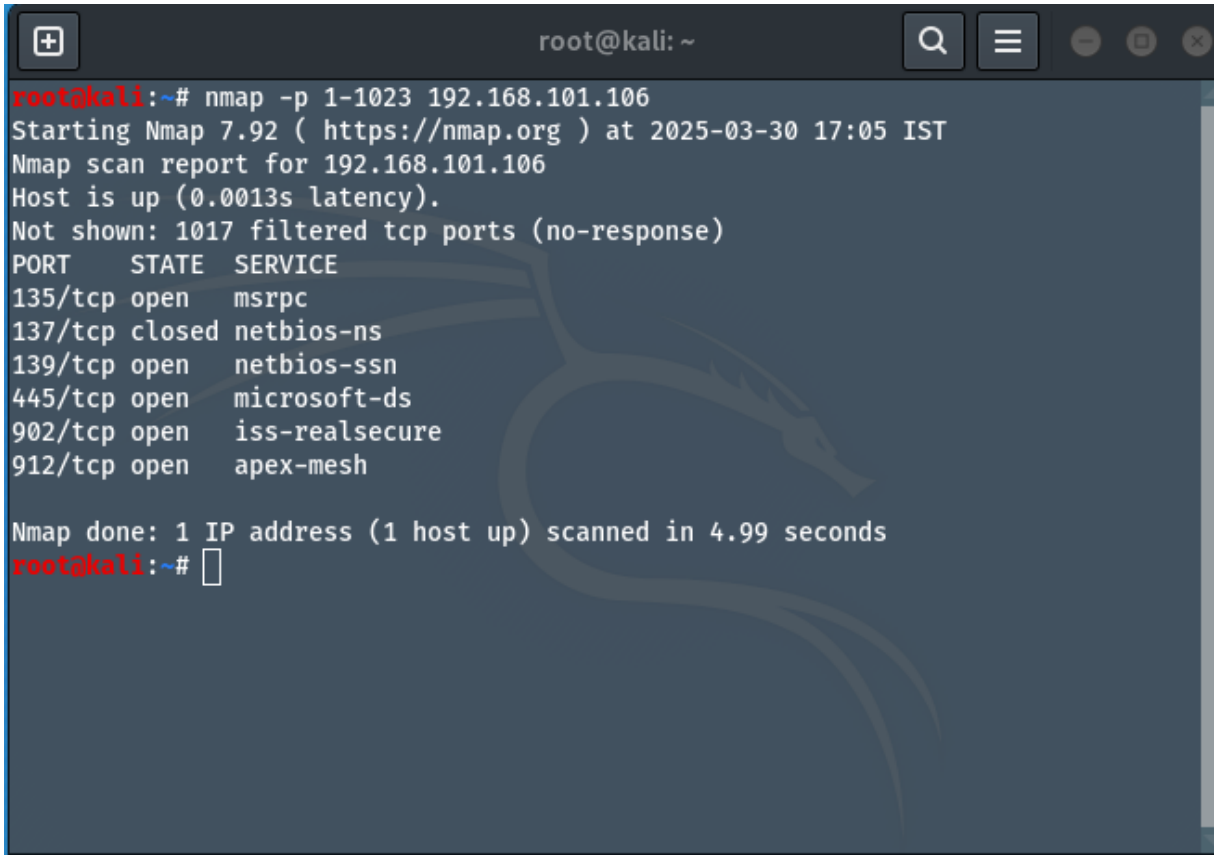
Nmap

Nmap is included with kali Linux and is available Graphic User Interface (GUI). After entering the target IP address and then clicking on the ‘scan’, all the details about the ports are shown.

Command used – *sudo nmap -p port_range target_ipaddress*

Figure 13 illustrates the results of a port scan performed using Nmap.

Figure 13 Port scanning using Nmap



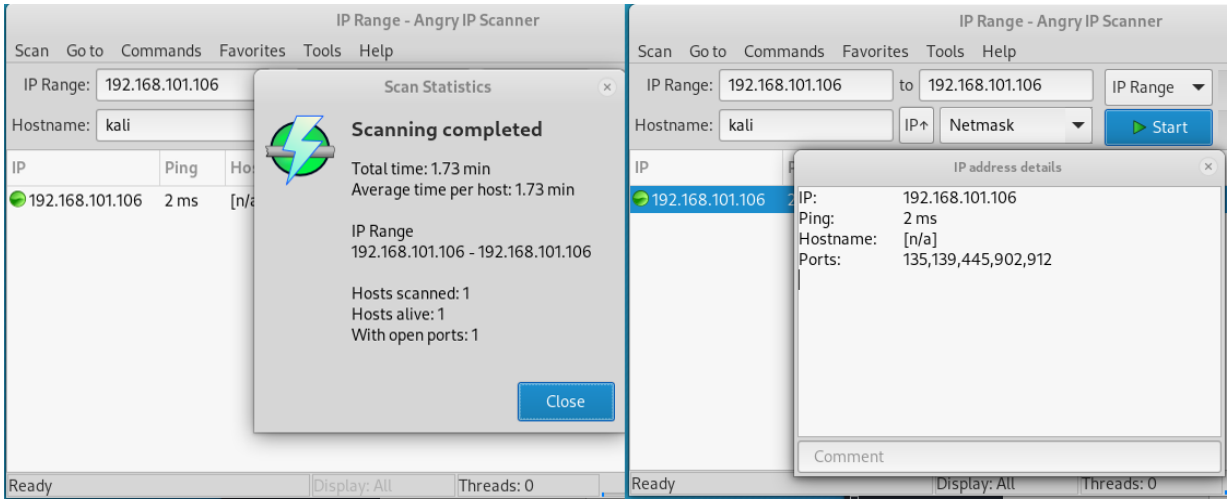
Angry IP Scanner

Angry IP scanner is not included in Kali Linux; .deb package is downloaded and can be installed running following command from the folder where .deb package is downloaded.

dpkg -i xxxx.deb

Once it is installed it can be run from Application menu. GUI makes it very easy to use, once target IP address is entered with IP mask and clicked 'Start', it starts to scan and 'Scan Statistics'. Figure 14 illustrates the results of a port scan performed using Angry IP Scanner.

Figure 14 Scanning port using Angry IP Scanner



Legion

As Legion was forked from Sparta and is not included in Kali Linux. It can be downloaded with simple command as a root.

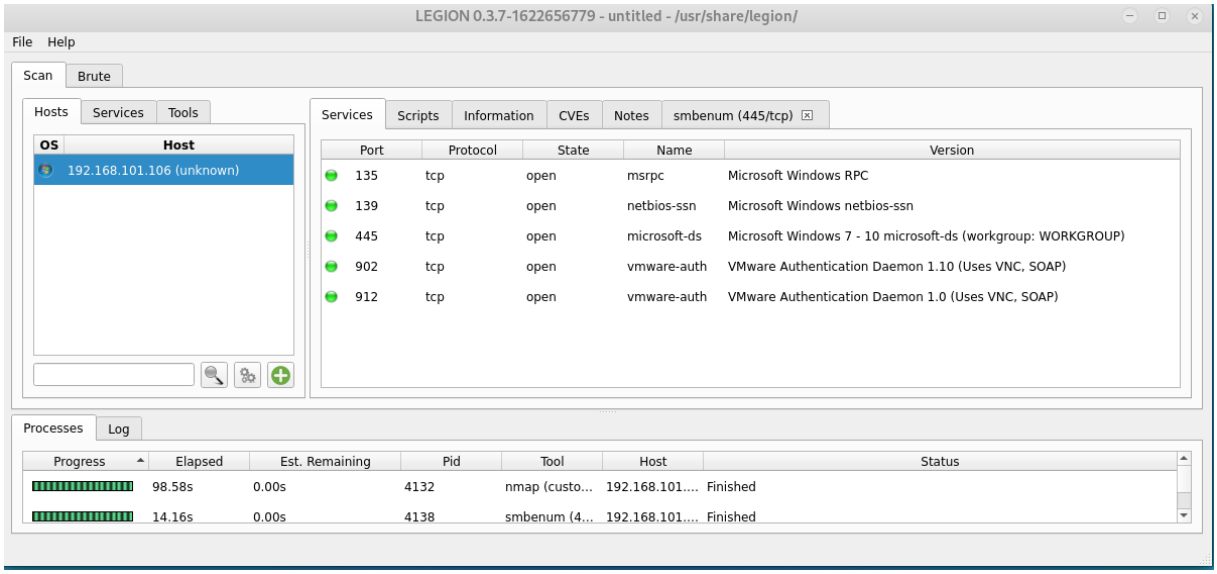
sudo apt install legion -y

With customizing arguments filed it was easy to set the port range.

-p 1-1023 -sV -O

GUI of the legion is simple and easy with various inbuilt features. Once the target IP address is entered with easy mode, ports are scanned. Figure 15 illustrates the results of a port scan performed using Legion.

Figure 15 Scanning port using Legion

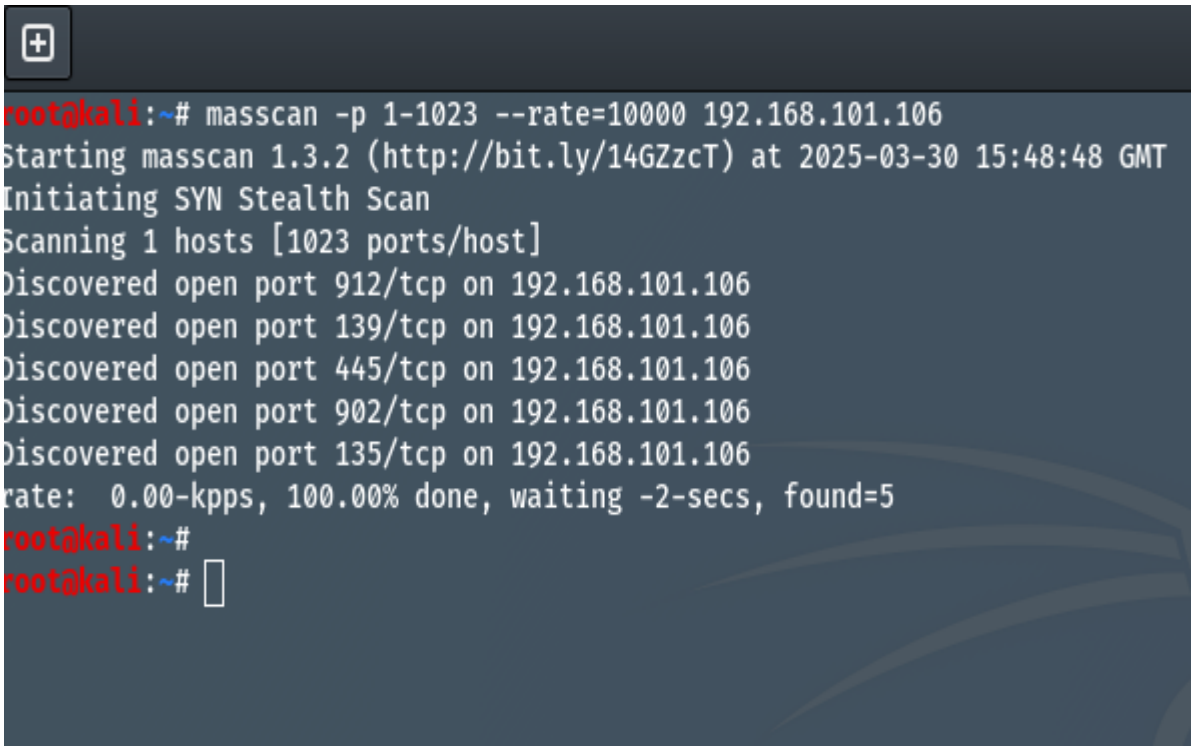


Masscan

Masscan can be downloaded from https://sourceforge.net/projects/masscan.mirror/ or can be cloned from the GitHub.

Figure 16 illustrates the results of a port scan performed using Masscan.

Figure 16 Port scanning using Masscan



Metasploit

Metasploit can be downloaded from Metasploit's official page.

start Metasploit – msfconsole

use TCP SYN port scanner – *use auxiliary/scanner/portscan/syn*

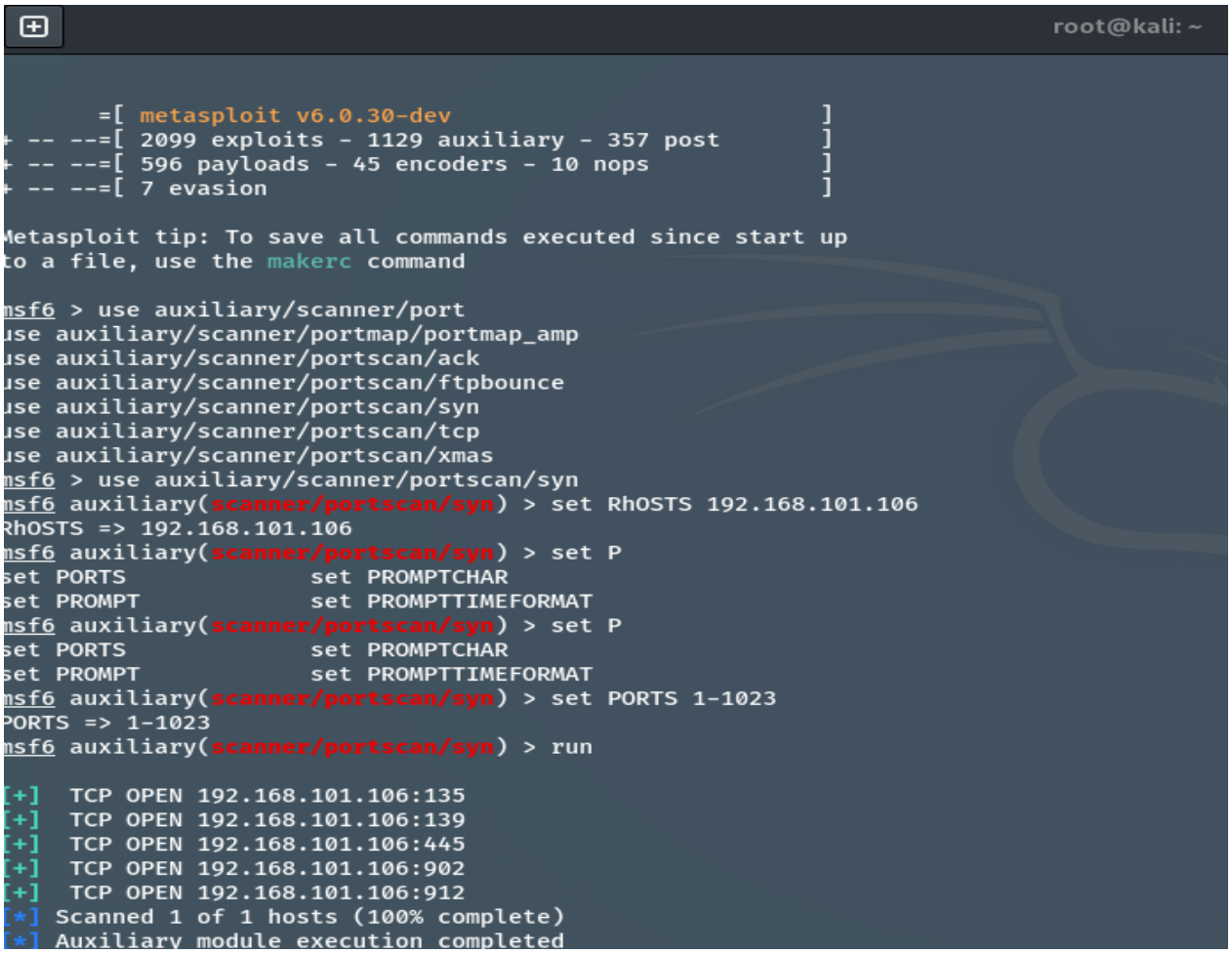
target IP address – *set RHOSTS [IP_address]*

set port range – *set PORTS 1-1023*

run the scan – *run*

Figure 17 illustrates the results of a port scan performed using Metasploit.

Figure 17 Port scanning using Metasploit



Findings

Nmap has various features and is very powerful and can be run through commands and used according to the need. Port scanning tools Legion is very simple and has a user-friendly GUI. Legion also comes with different features and is very easy to analyse.

6 Recommendations and Good Practices in SME

SMEs have been the main target of cyber-attacks and increasing at a higher rate recently. One of the main reasons we found out was the budget issues and lack of cyber security awareness knowledge in the organization. In most cases, organizations are not aware of cyber-attacks, and they do not realize that they have been the victim of cyber-attacks. With these misunderstandings and a lack of awareness about cyber security attacks, SMEs do not have proper plans and strategies to address those threats. As more and more businesses go online, smaller companies (SMEs) are at greater risk of cyber-attacks that could hurt their operations, steal their data, and damage their reputation. To address these threats, SMEs can use cyber security frameworks. These frameworks are like roadmaps that provide clear instructions and recommended practices for building strong security.

6.1 Cyber Security Frameworks

This section will discuss some important cybersecurity frameworks.

1. NIST Cyber security Frameworks (CSF):
   NIST Cyber Security Framework (NIST CSF) is being used by many small and mid-sized enterprises (SMEs) to help them deal with the ever-increasing threat landscape. The National Institute of Standards and Technology in the United States created this framework, which is well-liked due to its adaptable methodology [59]. The NIST CSF divides cyber security risk management into five essential steps, identify, protect, detect, respond, and recover. This contrasts with a one-size-fits-all approach. SMEs can obtain a comprehensive understanding of their present cyber security defenses by completing these steps. This enables them to identify potential weak points and set investment priorities to improve their overall security posture. In the end, the NIST CSF helps SMEs strengthen their defenses against cyber-attacks so they can recover more quickly if a breach occurs.

2. Coordinated Malware Eradication and Remediation Platform (CMERP)
   NIST A suitable Coordinated Malware Eradication and Remediation Platform (CMERP) framework that can be used against malware threats such as viruses, illegal crypto mining, and ransomware in an SME has been discussed and it has been used

as a base framework with the combination of NIST. The framework suggested in [32] consists of 5 main phases.

3. ISO/IEC 27001:
   ISO/IEC 27701 constitutes a significant augmentation of ISO 27001/2 within the context of compliance with the General Data Protection Regulation (GDPR) and the broader domain of data privacy. This enhancement transitions the Information Security Management System (ISMS) into a Privacy Information Management System (PIMS), thereby evidencing compliance with the GDPR as the organization manages both its own private data and that of third parties in a manner that adheres to regulatory standards. Nevertheless, it is imperative to acknowledge that this extension of ISO 27001/2 necessitates the prior implementation of the ISO 27001/2 framework as a foundational requirement [60].

4. Center for Internet Security (CIS) Controls:
   The Center for Internet Security (CIS) Controls is a set of best cyber security practices designed to help organizations prioritize and implement essential security measures. Each of the 20 CIS controls is further sub -divided into sub-controls, and in total there are 171 sub-controls across all 20 controls. The 20 controls are divided into three groups, basic, fundamental and organizational [61]. Small and medium enterprises (SMEs) can utilize CIS Controls to establish a fundamental security framework and progressively enhance their cyber security defenses.

5. European Union Agency for Cyber security (ENISA) Guidelines:
   For SMEs doing business in the EU, the European Union Agency for Cyber Security (ENISA) offers recommendations and guidelines to address several cyber security topics, such as incident response, risk management, and adherence to EU laws like the General Data Protection Regulation (GDPR) [24]. SMEs can improve their cyber security posture and guarantee adherence to EU cyber security standards by utilizing ENISA guidelines.

6. COBIT
   COBIT represents an additional framework that emphasizes the domain of auditing and information technology governance. Its primary objective is to ensure the

alignment of an organization's IT practices with its overarching strategic objectives [60]. Nonetheless, the difficulties encountered in the application of this framework are analogous to those observed in preceding frameworks. The framework is notably extensive, which may pose implementation challenges for smaller enterprises due to the necessity of defining numerous critical indicators such as stakeholders, scope, and objectives.

The article points out that existing cybersecurity frameworks such as NIST CSF, CMERP, ISO/IEC 27001, CIS Controls, ENISA Guidelines, and COBIT offer useful guidance but often do not meet the unique requirements of Small and Medium Enterprises (SMEs) [62]. These frameworks are usually crafted with larger organizations in mind, which means they require considerable resources, expertise, and financial commitment that most SMEs do not possess. This results in a disconnect, leaving SMEs at a disadvantage in implementing effective cybersecurity strategies.

To remedy this situation, the authors introduce the Least Cybersecurity Controls Implementation (LCCI) framework. The LCCI framework is designed specifically for SMEs, offering a phased approach that starts with fundamental cybersecurity controls and gradually enhances maturity. It focuses on prioritizing controls according to the specific sector and mission-critical assets of the SME, ensuring that security initiatives align with their most vital needs and available resources.

Researchers have posited that small and medium-sized businesses (SMBs) ought to direct greater attention towards strategies aimed at mitigating the repercussions of cyber-attacks, including the allocation of resources towards establishing an inspection team and formulating a comprehensive recovery plan [59]. Many small and medium-sized enterprises (SMEs) are supported by technology vendors for their hardware and software as they often lack the expertise and access to specialized knowledge [63]. There exist shared security obligations for both the vendor and the SME customer such as cloud-based Software-as-a-Service (SaaS). Good cyber security practices that are recommended in “A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations” is pointed out in the list below [59] : -

1) Allocating budgets for cyber security
2) Create password policies
3) Perform vulnerability assessments
4) Develop a strategy of training employees
5) Invest in and sufficiently train staff
6) Have regular awareness training
7) Make cyber security an agenda topic for boards
8) Treat cyber security like any other business risk
9) Develop a cyberattack response plan
10) Grow cyber security as the business grows
11) Perform a risk management assessment
12) Develop and document an internal IT security or cyber security policy
13) Have simple, clear policies
14) Ensure employees are familiar with the security policy
15) Take inventory of software
16) Ensure regular updates and patches of software
17) Perform automatic backups of all data
18) Securely backup business-critical data, such as customer data and financial information
19) Ensure backups can be restored when required
20) Use multi-factor authentication
21) Implement access control
22) Use passphrases in lieu of passwords
23) Invest in effective firewalls
24) Implement anti-virus and anti-malware
25) Install antivirus countermeasures on mobile platforms
26) Review contracts and policies with suppliers

27) Ensure suppliers have an accredited standard for cyber security for themselves and their partners to protect the supply chain

28) Have an up-to-date incident response plan

29) Practiced incident response plan regularly so that employees know what to do when they suspect there is an attempted breach or if an actual incident occurs

30) Consider investing in cyber insurance to cover the exposure of data privacy and security

31) Hire trustworthy employees

32) Secure remote access

33) Utilize encryption software

34) Employ dedicated cyber security staff

35) Implement multi-factor authentication

7 Conclusion

In conclusion, this master's thesis has explored the important topic of penetration testing in small and medium-sized businesses (SMEs), showing how crucial it is for protecting against cyber threats. SMEs must take proactive measures to protect their digital assets since they are becoming more and more of a target for cybercriminals because of their limited resources and frequently insufficient security measures. This study demonstrated how ethical hacking gives SMEs a crucial tool to successfully counteract cyber threats by locating and fixing vulnerabilities before they can be exploited.

This thesis explains by going over the idea of ethical hacking, highlighting its difficulties, moral dilemmas, and the significance of precise rules and industry standards of ethical hackers. Penetration testing frequently raises ethical concerns, which emphasizes the need to make sure these practices stay within moral and legal bounds while offering organizations real advantages. The thesis emphasized the benefits and drawbacks of this preventive security measure by examining the penetration testing procedure and its different forms. Along with providing insights into how these issues can be resolved, it also concentrated on the unique challenges that SMEs encounter when trying to implement penetration testing, such as a lack of resources and expertise.

A thorough analysis of the literature on cyber security gave researchers a thorough grasp of the risks that SMEs face as well as possible ways to reduce them. The study underlined how crucial it is for SMEs to improve their security posture by utilizing open-source tools as affordable solutions. SMEs can find and fix security flaws with the help of these tools, which include web penetration testing tools, network scanning tools, and vulnerability assessment tools. Although the functionality and focus of these tools differ, the study showed that SMEs could create a more secure network environment by carefully combining the appropriate tools.

The value of cyber security frameworks designed especially for SMEs was also examined in the thesis. By offering structured approaches for risk management, ongoing monitoring, and response planning, these frameworks help SMEs efficiently prioritize their cyber security initiatives. SMEs can strengthen their organization’s security culture, increase their resistance to changing threats, and protect sensitive data by implementing such frameworks.

This thesis’s research methodology focused on reviewing literature to comprehend the cyber security hurdles that are often faced by SMEs. From this perspective, it became apparent that

most of the time SMEs do face limitations and deficits of technical competencies but also have several tools and patterns that help them reinforce their defenses. The aim of the study's analysis of available tools and resources was to assist SMEs in enhancing their security systems such that even those with low resources can afford to do so.

The thesis emphasized the significance of continuing research and education in cyber security for SMEs in addition to offering tool recommendations. Staying ahead of new trends and technologies is essential for researchers, practitioners, and policymakers as cyber threats continue to increase in sophistication and frequency. This entails creating increasingly sophisticated tools, improving training curricula suited to SME's requirements, and figuring out more effective methods to incorporate cybersecurity procedures into their day-to-day operations.

In the end, this thesis acts as a useful manual for SMEs attempting to negotiate the complex world of cyber security. SMEs can greatly strengthen their defenses and reduce the risks they face by combining penetration testing, ethical hacking, and the strategic application of open-source tools and cyber security frameworks. The information in this thesis offers best practices and practical insights, giving SMEs the information and resources they need to safeguard themselves in a world that is becoming more and more digital.

In conclusion, SMEs have a variety of useful and affordable options that can help them protect their operations, even though they still face substantial cybersecurity challenges. SMEs can lessen their susceptibility to cyber-attacks, safeguard their private information, and establish a safe environment for their companies to flourish by embracing ethical hacking techniques, utilizing open-source tools, and putting strong cyber security frameworks in place. Overall, this thesis provides a helpful guide for SMEs navigating the complex world of cyber security. It offers practical tips and best practices based on thorough research and analysis. As cyber-attacks on SMEs continue to rise, the information in this thesis is vital for helping them stay safe and protect their sensitive data. To keep SMEs resilient and ready for the challenges that lie ahead, ongoing research and innovation will be crucial as cyber threats change.

7.1 Future Research

In the field of penetration testing for SMEs, several interesting areas become obvious. Exploration of cutting-edge penetration testing methods, such as incorporating machine learning and artificial intelligence algorithms to improve accuracy and efficiency in identifying

complex cyber threats, is one approach. To streamline the testing process and make it more accessible to businesses with limited resources, it is also necessary to investigate the creation of automated penetration testing tools designed especially for SMEs. Examining how penetration testing can be incorporated into DevSecOps pipelines to strengthen security posture and reduce vulnerabilities in SMEs' systems and applications is another exciting field.

Furthermore, future research could explore the impact of regulatory compliance requirements on penetration testing practices within SMEs and evaluate the effectiveness of cyber security awareness and training programs in empowering SMEs to better understand and respond to cyber threats. Another crucial area that requires further research is how open-source penetration testing tools can lower expenses and make strong cyber security measures more accessible to SMEs.

To improve cyber security resilience in this crucial industry, case studies and longitudinal research may offer insightful information about typical obstacles, success factors, and best practices for penetration test implementation in SMEs. Furthermore, the scalability and adaptability of current penetration testing frameworks to the unique requirements of SMEs operating in various industries or geographical areas must be assessed. To create more efficient methods for carrying out and implementing penetration-testing procedures, cooperative projects involving SMEs, and governmental organizations could also be investigated. Finally, encouraging broad adoption among SMEs with limited resources will require an awareness of how penetration-testing solutions strike a balance between cost, efficacy, and simplicity of use.

8 References

[1] IBM, “Cost of a Data Breach Report 2024,” 2024.

[2] European Commission, “EUR-Lex - 32003H0361 - EN - EUR-Lex.” Accessed: Mar. 17, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reco/2003/361/oj

[3] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[4] W. N. Abidde, N. Eyidia, and E. S. J. Eme, “CIA TRIAD: A REVIEW OF THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF DATA IN A SYSTEM OF CONNECTED NETWORKS,” *www.irjmets.com @International Research Journal of Modernization in Engineering*, 1282, doi: 10.56726/IRJMETS68704.

[5] A. G. Bacudio, X. Yuan, B. T. Bill Chu, and M. Jones, “An Overview of Penetration Testing,” *International Journal of Network Security & Its Applications*, vol. 3, no. 6, pp. 19–38, Nov. 2011, doi: 10.5121/ijnsa.2011.3602.

[6] J. P. Mcdermott, “Attack Net Penetration Testing.”

[7] I. Yaqoob, S. A. Hussain, S. Mamoon, N. Naseer, J. Akram, and A. Ur Rehman, “Penetration Testing and Vulnerability Assessment,” *Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org*, vol. 7, no. 8, 2017, [Online]. Available: www.jncet.org

[8] S. A. Saleem, “Ethical Hacking as a risk management technique,” 2006. [Online]. Available: http://www.research.ibm.com/journal/sj/403/palmer.html.

[9] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, “A Survey on Ethical Hacking: Issues and Challenges,” Mar. 2021, [Online]. Available: http://arxiv.org/abs/2103.15072

[10] M. J. Carey *et al.*, “Data-Centric Systems and Applications Series Editors.”

[11] B. Rafferty, “Dangerous skills gap leaves organisations vulnerable,” *Network Security*, vol. 2016, no. 8, pp. 11–13, Aug. 2016, doi: 10.1016/S1353-4858(16)30077-0.

[12] J. Firch, “How To Perform A Successful Network Penetration Test | PurpleSec.” Accessed: Mar. 23, 2022. [Online]. Available: https://purplesec.us/network-penetration-test/#NetworkPenetrationTest

[13] H. M. Z. Al Shebli and B. D. Beheshti, “A study on penetration testing process and tools,” in *2018 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2018*, Institute of Electrical and Electronics Engineers Inc., Jun. 2018, pp. 1–7. doi: 10.1109/LISAT.2018.8378035.

[14] T. Parmesivan and M. F. Zolkipli, “Study on issues and challenges onadvancement of Penetration Testing,” *International Journal of Advances in Engineering and Management (IJAEM)*, vol. 4, p. 983, 2022, doi: 10.35629/5252-0403983986.

[15] M. Alhamed and M. M. H. Rahman, “A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions,” Jun. 01, 2023, *MDPI*. doi: 10.3390/app13126986.

[16] Adebola Folorunso, Ifeoluwa Wada, Bunmi Samuel, and Viqaruddin Mohammed, “Security compliance and its implication for cybersecurity,” *World Journal of Advanced Research and Reviews*, vol. 24, no. 1, pp. 2105–2121, Oct. 2024, doi: 10.30574/wjarr.2024.24.1.3170.

[17] J. Saleem, B. Adebisi, R. Ande, and M. Hammoudeh, “A state of the art survey - Impact of cyber attacks on SME’s,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jul. 2017. doi: 10.1145/3102304.3109812.

[18] M. Heikkila, A. Rattya, S. Pieska, and J. Jamsa, “Security challenges in small-and medium-sized manufacturing enterprises,” in *2016 International Symposium on Small-Scale Intelligent Manufacturing Systems, SIMS 2016*, Institute of Electrical and Electronics Engineers Inc., Dec. 2016, pp. 25–30. doi: 10.1109/SIMS.2016.7802895.

[19] A. Da Veiga and N. Martins, “Improving the information security culture through monitoring and implementation actions illustrated through a case study,” *Comput Secur*, vol. 49, pp. 162–176, 2015, doi: 10.1016/j.cose.2014.12.006.

[20] IBM, “data-security.” Accessed: May 05, 2023. [Online]. Available: https://www.ibm.com/topics/data-security

[21] A. M. Y. Chu and P. Y. K. Chau, “Development and validation of instruments of information security deviant behavior,” *Decis Support Syst*, vol. 66, pp. 93–101, 2014, doi: 10.1016/j.dss.2014.06.008.

[22] D.-G. for M. and H. A. Ipsos European Public Affairs at the request of the European Commission, “Report Flash Eurobarometer 496 - SMEs and cybercrime,” 2021, doi: 10.2837/14988.

[23] ESET, “ESET SMB Cybersecurity Report 2024,” 2024.

[24] E. European Union Agency for Cybersecurity, “CYBERSECURITY FOR SMES Challenges and Recommendations CYBERSECURITY FOR SMES ABOUT ENISA,” 2021, doi: 10.2824/770352.

[25] D. Ghelani, “Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review,” Sep. 22, 2022. doi: 10.22541/au.166385207.73483369/v1.

[26] M. M. Tiwari, R. Kumar, A. Bharti, and J. Kishan, “INTRUSION DETECTION SYSTEM,” 2017. [Online]. Available: www.ijtra.com,

[27] C. Rombaldo, I. Becker, S. Johnson, and C. Rombaldo Junior, “Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity,” 2023.

[28] A. B. A. Ali, R. K. Ayyasamy, R. Akbar, V. A. Ponnusamy, and L. E. Heng, “Cybersecurity Infrastructure adoption Model for Malware Mitigation in Small Medium Enterprises (SME),” in *2022 IEEE 5th International Symposium in Robotics and Manufacturing Automation, ROMA*

2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ROMA55875.2022.9915696.

[29] H. M. T. N. Jayathilaka and J. Wijayanayake, "Systematic Literature Review on Developing an AI Framework for SME Cybersecurity Identification and Personalized Recommendations," *Journal of Desk Research Review and Analysis*, vol. 2, no. 2, pp. 249–250, Jan. 2025, doi: 10.4038/jdrra.v2i2.53.

[30] A. Emer, M. Unterhofer, and E. Rauch, "A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises," *IEEE Engineering Management Review*, vol. 49, no. 2, pp. 98–109, Apr. 2021, doi: 10.1109/EMR.2021.3078077.

[31] G. Taskin and M. T. Sandikkaya, "Comparison of Security Frameworks for SMEs," in *14th International Conference on Electrical and Electronics Engineering, ELECO 2023 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ELECO60389.2023.10416030.

[32] M. M. A. Mutalib, Z. Zainol, and M. H. M. Halip, "Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework," in *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICRAIE52900.2021.9703991.

[33] A. Alexei and A. Alexei, "The problem of information systems security in SME," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Sep. 2023, pp. 101–105. doi: 10.1145/3603304.3603346.

[34] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *PLoS One*, vol. 19, no. 3 March, Mar. 2024, doi: 10.1371/journal.pone.0301183.

[35] L. Ambreen, M. Jain, R. K. Yadav, and S. Loonkar, "Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review," *Multidisciplinary Reviews*, vol. 6, 2023, doi: 10.31893/multirev.2023ss080.

[36] R. Khan, M. Tech, and M. Hasan, "NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 8, pp. 116–120, 2017, doi: 10.26483/ijarcs.v8i8.4641.

[37] H. Berger and A. Jones, "Cyber security & ethical hacking for SMEs," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jul. 2016. doi: 10.1145/2925995.2926016.

[38] Cisco, "Cyber Attack - What Are Common Cyberthreats? - Cisco." Accessed: Jul. 10, 2022. [Online]. Available: https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~how-cyber-attacks-work

[39] I. Fernandez De Arroyabe and J. C. Fernandez de Arroyabe, “The severity and effects of Cyber-breaches in SMEs: a machine learning approach,” *Enterp Inf Syst*, 2021, doi: 10.1080/17517575.2021.1942997.

[40] OWASP, “OWASP ZAP – Getting Started.” Accessed: Aug. 16, 2022. [Online]. Available: https://www.zaproxy.org/getting-started/

[41] Offensive Security, “skipfish | Kali Linux Tools.” Accessed: Apr. 05, 2025. [Online]. Available: https://www.kali.org/tools/skipfish/

[42] N. Surribas, “GitHub - wapiti-scanner/wapiti: Web vulnerability scanner written in Python3.” Accessed: Apr. 05, 2025. [Online]. Available: https://github.com/wapiti-scanner/wapiti

[43] T. “Zapotek” Laskos, “GitHub - Arachni/arachni: Web Application Security Scanner Framework.” Accessed: Apr. 05, 2025. [Online]. Available: https://github.com/Arachni/arachni

[44] W. Alcorn, “BeEF - The Browser Exploitation Framework Project.” Accessed: Aug. 16, 2022. [Online]. Available: https://beefproject.com/

[45] PortSwigger Ltd., “Burp Suite - Application Security Testing Software - PortSwigger.” Accessed: Apr. 05, 2025. [Online]. Available: https://portswigger.net/burp

[46] J. Wack, M. Tracy, M. Souppaya, and A. L. Bement, “Guideline on Network Security Testing Recommendations of the National Institute of Standards and Technology,” 2003.

[47] G. Giacobbi, “The GNU Netcat -- Official homepage.” Accessed: Aug. 16, 2022. [Online]. Available: http://netcat.sourceforge.net/

[48] A. Keks, “Angry IP Scanner - the original IP scanner for Windows, Mac and Linux.” Accessed: Aug. 16, 2022. [Online]. Available: https://angryip.org/

[49] Offensive Security, “Kali Linux / Packages / legion · GitLab.” Accessed: Apr. 05, 2025. [Online]. Available: https://gitlab.com/kalilinux/packages/legion

[50] Rapid7, “Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit.” Accessed: Apr. 05, 2025. [Online]. Available: https://www.metasploit.com/

[51] R. D. Graham, “GitHub - robertdavidgraham/masscan: TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.” Accessed: Apr. 05, 2025. [Online]. Available: https://github.com/robertdavidgraham/masscan

[52] A. (Solar D. Peslyak, “John the Ripper password cracker.” Accessed: Apr. 05, 2025. [Online]. Available: https://www.openwall.com/john/

[53] T. d’Otreppe Bériot, “Aircrack-ng.” Accessed: Apr. 05, 2025. [Online]. Available: https://www.aircrack-ng.org/

[54] Inc. Tenable, “Tenable Nessus Essentials Vulnerability Scanner | Tenable®.” Accessed: Apr. 05, 2025. [Online]. Available: https://www.tenable.com/products/nessus/nessus-essentials

[55] M. Heuse, “GitHub - vanhauser-thc/thc-hydra: hydra.” Accessed: Apr. 05, 2025. [Online]. Available: https://github.com/vanhauser-thc/thc-hydra

[56] Greenbone Networks GmbH, “OpenVAS - Open Vulnerability Assessment Scanner.” Accessed: Aug. 16, 2022. [Online]. Available: https://openvas.org/

[57] Inc. Cisco Systems, “Snort - Network Intrusion Detection & Prevention System.” Accessed: Aug. 15, 2022. [Online]. Available: https://www.snort.org/

[58] Atomicorp, “OSSEC - Open Source HIDS - FIM, Rootkit Detection, Malware Detection.” Accessed: Aug. 15, 2022. [Online]. Available: https://www.ossec.net/about/

[59] A. Chidukwani, S. Zander, and P. Koutsakis, “A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations,” *IEEE Access*, vol. 10, pp. 85701–85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[60] M. El-Hajj and Z. A. Mirza, “ProtectingSmall and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool,” *Electronics (Switzerland)*, vol. 13, no. 19, Oct. 2024, doi: 10.3390/electronics13193910.

[61] S. Gros, “A Critical View on CIS Controls,” in *Proceedings of the 16th International Conference on Telecommunications, ConTEL 2021*, Institute of Electrical and Electronics Engineers Inc., Jun. 2021, pp. 122–128. doi: 10.23919/ConTEL52528.2021.9495982.

[62] S. Pawar and D. H. Palivela, “LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs),” *International Journal of Information Management Data Insights*, vol. 2, no. 1, Apr. 2022, doi: 10.1016/j.jjimei.2022.100080.

[63] P. A. H. Williams, “Small Business-A Cyber Resilience Vulnerability,” 2012. [Online]. Available: https://www.researchgate.net/publication/49285574