applied sciences

MDPI

Review

A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions

Mariam Alhamed * and M. M. Hafizur Rahman *

Department of Computer Networks and Communications, CCSIT, King Faisal University, Al-Ahsa 31982, Saudi Arabia

* Correspondence: 222402149@student.kfu.edu.sa (M.A.); mhrahman@kfu.edu.sa (M.M.H.R.)

Abstract: Given the widespread use of the internet at the individual, governmental, and nongovernmental levels, and the opportunities it offers, such as online shopping, security concerns may arise. Cyber criminals are responsible for stopping organizations' access to internet, for stealing valuable and confidential data, and causing other damage. Therefore, the network must be protected and meet security requirements. Network penetration testing is a type of security assessment used to find risk areas and vulnerabilities that threaten the security of a network. Thus, network penetration testing is designed to provide prevention and detection controls against attacks in the network. A tester looks for security issues in the network operation, design, or implementation of the particular company or organization. Thus, it is important to identify the vulnerabilities and identify the threats that may exploit them in order to find ways to reduce their dangers.The ports at risk are named and discussed in this study. Furthermore, we discuss the most common tools used for network penetration testing. Moreover, we look at potential attacks and typical remediation strategies that can be used to protect the vulnerable ports by reviewing the related publications. In conclusion, it is recommended that researchers in this field focus on automated network penetration testing. In the future, we will use machine learning in WLAN penetration testing, which provides new insight and high efficiency in performance. Moreover, we will train machine learning models to detect a wide range of vulnerabilities in order to find solutions to mitigate the risks in a short amount of time rather that through manual WLAN penetration testing, which consumes a lot of time. This will lead to improving security and reducing loss prevention.

Keywords: penetration testing; network penetration testing; vulnerabilities; attack

Citation: Alhamed, M.; Rahman, M.M.H. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Appl. Sci.* **2023**, *13*, 6986. https://doi.org/10.3390/app13126986

Academic Editor: Luis Javier Garcia Villalba

Received: 27 April 2023
Revised: 21 May 2023
Accepted: 22 May 2023
Published: 9 June 2023

1. Introduction

We currently live in the age of technology, which is integrated into our daily lives and is based on the internet. Technology makes it easy for its users to perform activities online. Although technology offers many conveniences and opportunities, it has some risks such as cyber attacks. These risks are due to aggressive competition between commercial and non-commercial organizations that use networks to deliver services.

In order to deliver services, we need open ports in networks. A TCP or UDP port number that is open accepts packets, while a closed port denies connections or ignores all communication. Ports are used for all internet communications. Consequently, certain ports are required for internet-based services to receive and transmit data. If the service listening on the port is misconfigured, unpatched, vulnerable to attack, or has inadequate network security controls, open ports can pose a risk and are referred to as vulnerable ports [1].

We have found that it is easy to exploit any vulnerabilities in order to implement any type of attack. Therefore, many individuals and organizations are affected by this attack, which leads to the shutdown of individuals' networks and organizations' websites. For example, around 500 Coop supermarkets in Sweden had to close in 2021. The reason for this was because of a ransomware hack that hit businesses around the world. Late Sunday, the hackers demanded USD 70 million to release the encrypted files the ransomware was

holding. Coop did not respond and their payment service provider was obliged to manually restore the payment terminals in each store using backups to fix the problems [2].

To prevent these attacks, organizations use tests called penetration tests. These are referred to as ethical hacking and white hat attacks. Penetration testing is a method of identifying security vulnerabilities in networks, applications, and computer systems that can be exploited by attackers.

Penetration testing is a proactive way to identify vulnerabilities in digital assets by actively looking for vulnerabilities and exploiting them from the attacker's perspective. To achieve the cyber security objectives, which are integrity, availability, and confidentiality in the modern digital environment, penetration testing has become a mandatory element, especially with the introduction of the European General Data Protection Regulation for institutions and enterprises. Today, there are varieties of options for penetration testing. There are a variety of systems with tools that perform penetration testing including Kali Linux with such security tools as Nmap.

Penetration tests are used to detect the vulnerabilities present in the system and to know how to eliminate them. They simulate different types of attacks on the target system. Through these tests, the tester can identify the vulnerabilities in an organized and controlled manner. Thus, they create reports of the problems requiring system repair and patch security vulnerabilities to the management. This is considered to be a risk assessment and can be used to verify network security. Penetration testing is very important for organizations but the resources are costly and time consuming. Therefore, a specialized penetration testing technique is needed to protect systems and devices and to ensure information and network security in a fast and inexpensive way. The use of the internet has become widespread. Therefore, data security is very important to prevent the attempts of cyber criminals. Prior to the criminals' attempt to exploit the vulnerabilities in a network, the specialists will have conducted penetration tests to detect and fix the vulnerabilities. A network can be an IoT network, LAN, WLAN, or WAN.

The network penetration test is an ethical precaution designed to identify the risks that may occur if an attacker gains access to the company's computer systems and networks. In addition, it is an authorized simulated cyber attack that helps to create a plan to address security vulnerabilities in the IT infrastructure before the actual attack occurs. It is carried out by trained security experts, so-called ethical hackers [1].

Thus, the purpose of network penetration testing is to protect data and ensure overall security, especially when it comes to managing important data. Examples include SQL injections, inadequately configured firewalls, and traditional viruses or malware. In addition, certain regulations insist on network penetration testing and continuous maintenance to ensure long-term security [3].

This paper aims to raise awareness and improve the technique of network penetration testing. In addition, this paper will help raise awareness among organizations that have been or may be victims of cyber crime due to their employees' use of technology.

1.1. Types of Penetration Tests

Several authors have outlined that there are three approaches to penetration testing [4]. The most common approaches include black box, white box, and gray box testing.

1.1.1. Black Box

According to Jayasuryapal [4], in black box testing, testers simulate an attack without any information about the infrastructure. In this way, the testers discover all vulnerabilities using their methods and tools. This means that the testers use a number of real attack techniques such as social engineering and remote access. For example, the testers obtain the IP address of the network without any other information. Then, the testers simulate all attack techniques to find all known and unknown vulnerabilities in the network. See Table 1.

1.1.2. White Box

According to Jayasuryapal [4], in white box testing, testers simulate the attack with complete information about the infrastructure, operating system details, IP address, and some passwords. It is designed to allow the testers to perform the attack using familiar knowledge about the target system of organizations such as the personal details of an internal employee. This preserves the integrity of the organization's network infrastructure and reduces the risk of an internal attacker, such as a disgruntled employee. See Table 1.

1.1.3. Gray Box

According to Jayasuryapal [4], the gray box approach is performed when the white and black boxes are combined and used together to capture the internal and external security information. In this way, the testers have some limited information about the network infrastructure. Gray box testing eliminates the internal or external security issues that can be exploited by attackers [5]. See Table 1.

Table 1. The different penetration testing approaches.

	Black Box	**White Box**	**Gray Box**
Knowledge	Zero knowledge	Full knowledge	Some knowledge
Access level	Zero access testing as attacker.	Complete open access testing as developer.	Testing as user with access to part of the data.
Pros	It is more realistic.	More thorough, less likely to miss a vulnerability, and is faster. Intended for high-risk or sensitive data processing systems.	It is more efficient than a black box and saves both time and money.
Cons	It takes more time and increases the likelihood that a vulnerability will be missed.	More data must be delivered to the tester, which increases costs.	There are no significant disadvantages to this form of testing.

1.2. Impact of Hacking on Organizations and Governments

Due to the dominance of technology in the business world and governments, it has become important to protect this technology from attacks, as these organizations can put their customers' personal and financial information at risk. The attacks are often internal, such as by a disgruntled employee.

As a result, companies lose many billions due to electronic attacks, and they can also lose their reputation and the trust of their customers, and then they are held legally responsible for the loss of their customers.

The researchers of [6] pointed out that the financial losses are presented in the reports of the hacked companies, and they stated that in 2011, Sony had its PlayStation system hacked and lost about USD 170 million. Recovering this loss can be very difficult. Moreover, the researchers stated that piracy leads to the loss of information by deleting or modifying important files. In the last 10 years, the servers at the FBI, Interpol, and NASA have been attacked in different regions. Organizations that have been hacked pay a heavy price in terms of reputation damage. The reputation damage causes customers to think more carefully before working with a company that has been hacked because they fear for their personal information, and the company loses business over time because of the reputation damage. Therefore, what we are finding is that the need for IT security services has increased dramatically. Furthermore, the researchers of [6] stated that for organizations

and individuals, it is important to be aware of the risks and security, and penetration testing is one of the preventive measures in cyber security. In terms of the impact of hacking on the finances and reputation of organizations, we found that T-Mobile faced this impact significantly. On 1 May 2023, a data breach occurred at T-Mobile that affected about 800 of the telecommunications provider's customers, further damaging the company's reputation because it was not the first data breach that year. The first data breach took place in January and affected 37 million customers. In addition, T-Mobile was also affected in November 2022, costing the company USD 350 million. Therefore, the company must ensure that it secures its networks and raises awareness among its employees [7].

1.3. Standards of the Penetration Test

Cyber attackers always use different attack vectors on their victims due to the lack of effective policies and standards. Thus, they exploit the system and steal valuable information. To ward off cyber attackers, there are some standards used by penetration testers to prevent attacks. The common standards are [8]:

1.3.1. Information Systems Security Assessment Framework (ISAAF)

The goal of this standard is to evaluate the application, system, and network controls. There are three phases: [8]

- Planning and preparation;
- Assessment; and
- Reporting.

1.3.2. National Institute of Standards and Technology Special Publication 800-115 (NIST SP 800-115)

Guidelines for organizing and conducting information security testing and assessments are provided by the NIST standard (SP800-115). In addition, the results should be evaluated and mitigation plans established. It is not intended to be a comprehensive test or assessment but it is intended to provide an overview of the major components of security testing and assessments, focusing on specific methods and identifying their advantages and disadvantages. It also includes reports and recommendations for their use. According to the NIST standard (SP800-115), the penetration testing process can be divided into the following four steps: planning, detecting, attacking, and reporting [8].

1.3.3. Open-Source Security Testing Methodology Manual (OSSTMM)

To ensure the security of the network, this manual provides the best practices. Thus, this standard helps to provide an overview of the network's cyber security as well as the best solutions for the technological context to make the right decision to protect the network. This version was published in 2010 [8].

1.3.4. Penetration Testing Execution Standard (PTES)

Interactions before engagement: the standard ensures that users are prepared for the pentest. Everything revolves around the release of documents and test-related equipment:

- Gathering information;
- Threat modeling;
- Vulnerability analysis;
- Exploitation; and
- Reporting.

1.4. Penetration Testing Tools

Penetration testing involves simulating different types of attacks to identify the existing vulnerabilities in the system using different tools. These tools are very important and fundamental for testers. See Table 2 , Researchers have studied different tools including:

- Aircrack-ng is a complete suite of tools for evaluating the security of WiFi networks and focuses on different areas of WiFi security, which are detection, packet sniffing, WEP and WPA/WPA2-PSK cracking and analysis tool for 802.11 wireless LANs [6].
- Nmap is a network mapper which is used as penetration-testing tool to scan the network to identify ports, hosts, operating systems, and services to discover vulnerabilities. [4] It is used in the first phase of penetration testing. It is also suitable for scanning large and small networks. Nmap scans many type of protocols and existing systems [9].
- Metasploit is an open-source penetration tool that allows you to test vulnerabilities in operating systems and applications. It runs a set of codes on the test target. It creates a framework for penetration testing and works on Linux, Apple Mac OS X and Microsoft Windows [10].
- BeEF is Browser Exploitation Framework, which is used for the web browser. It works on Linux, Apple Mac OS X and Microsoft Windows. It examines exploitability in the context of web browsers [10].
- Shadow is a search engine that allows you to find specific devices and their types. It scans the entire Internet and then analyzes the banners returned by the scanned devices. The results are the versions of Web servers, anonymous FTP servers if they exist in a specific location, and information about the device's model [1].
- Nessus is a remote advance scan tool that used in penetration testing. It runs in one machine to scan the services offered by a remote machine. It is used in over 75,000 organizations world wide [10].
- Wireshark is an open source program that runs on UNIX, Windows and many other operating systems. It uses a graphical user interface and called network sniffer. It is a passive tool used for troubleshooting network problems. It analyzes and captures packet traffic without being detected by other parties [1].
- Zed Attack Proxy (ZAP) is a simple and free security solution that integrates penetration testing to detect vulnerabilities in web applications. For this reason, it is the best tool for developers and functional testers who are new to penetration testing, as it can be used by people with a wide range of security experience.
- Netcat is a command line tool that uses the TCP or UDP protocols to read and write data over network connections. It is one of the strongest weapons in the inventory of network and system administrators [11].

Table 2. Penetration Testing Tools.

Tool Name	Purpose	Portability
Nmap	It is used for: - Network Scanning; - Port Scanning; and - OS Detection.	It runs on Linux, Windows, FreeBSD, OS X, HP-UX, NetBSD, Sun, OpenBSD, Solaris, and Mac.
Metasploit Framework	It is used to create and execute exploit codes against a remote target. It is used to test the vulnerability of computer systems.	Any Windows and Unix version.
BeEF	It is used to exploit the cross-scripting XSS flaw in a web application.	It runs on Mac OSX 10.5.0 or modern Linux.

Table 2. *Cont.*

Tool Name	Purpose	Portability
Shadow Security Scanner	It is used to identify network errors and to check proxies.	Scan servers built on each platform.
Nessus	It is used to identify security vulnerabilities that allow hackers to remotely take over or access sensitive data.	It runs on Oracle Solaris, Mac OS X, Linux, Apple, FreeBSD, and Windows.
Wireshark	It is a network analyzer.	It runs on Windows, Linux, macOS, Solaris, FreeBSD, and NetBSD.
Zed Attack Proxy (ZAP)	It is used to detect vulnerabilities in web applications.	It runs on Windows, Linux, and Mac OS X.
Aircrack-ng	It is a tool used to assess Wi-Fi networks.	It runs primarily on Linux but also on Windows, macOS, Solaris, FreeBSD, OpenBSD, and NetBSD.
Netcat	It is a computer network tool.	It runs on Linux, macOS, Windows, and BSD.

1.5. Importance of Manual Penetration Testing versus Automated Penetration Testing

Computer systems are not intelligent enough to know exactly how developers should behave. Systems behave exactly the way developers program them. A business logic vulnerability occurs when developers make a logical error in their programs. Therefore, manual penetration testing that relies on humans is still necessary because it can uncover vulnerabilities that are missed by automated scanners. If requirements change and ongoing tests fail, the automated penetration test has failed but it has still passed because the old implementation is no longer viable. Moreover, manual penetration testing can handle requirement updates. It is also impossible to detect rare cases of vulnerabilities. The probability of false positives and false negatives is high. Therefore, manual penetration testing can uncover alternative security techniques used by developers, reducing the number of false positives in vulnerability detection [12].

Therefore, the goals of this study are as follows:

- To review the tools used for network penetration testing;
- To review network penetration testing methodologies;
- To identify all possible attacks on all open ports; and
- To review mitigation techniques used to protect open ports from threats.

The study is organized as follows: Section 2 describes the systematic literature review methodology. Section 3 is a literature review that presents the wireless local area network penetration testing and an example of wireless local area network penetration testing architecture and methodology. Section 4 summarizes the results and discussion. Section 5 offers recommendations for future research directions. Section 6 concludes the study.

2. Systematic Literature Review Methodology

This paper uses Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) to select the appropriate papers for analysis. In PRISMA, the research strings were first formatted as penetration testing AND network penetration testing, vulnerable

port in network OR network security. The search was applied to Google scholar and the Saudi Digital Library and focused on papers published between 2018 and 2022 and related to penetration testing. PRISMA consists of three phases, namely the identification phase, the screening phase, and the inclusion phase. First, in the identification phase, 504 duplicate records and 35,777 records were removed from the Google Scholar database for other reasons. In addition, 877 records were removed from the Saudi Digital Library (SDL). In the next phase, screening, 132 papers with duplicate data and 55 papers that contained only an abstract were removed. In addition, 789 papers with non-specific objectives and 106 papers unrelated to the topic were excluded, and three papers in a foreign language were removed. Finally, in the inclusion phase, 25 papers were selected from the Google Scholar database and 14 papers were selected from the Saudi Digital Library (SDL) (See Figure 1).

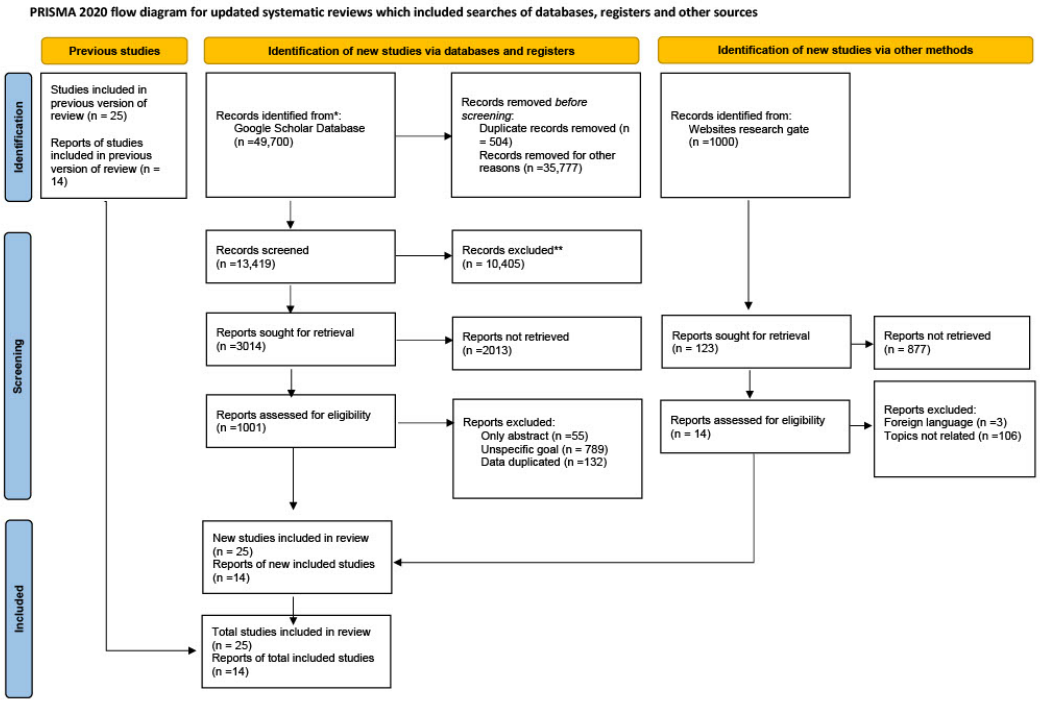

Figure 1. PRISMA literature review schematic. * Consider, if feasible to do so, reporting the number of records identified from each database or register searched (rather than the total number across all databases/registers). ** If automation tools were used, indicate how many records were excluded by a human and how many were excluded by automation tools.

Table 3 illustrates the publication years of the selected papers, with most of the selected articles were published in 2019.

Table 3. Publication Year of the selected papers.

Year	Number of Papers
2018	7 Papers
2019	11 Papers
2020	10 Papers
2021	4 Papers
2022	7 papers

3. Literature Review

The selected papers related to the penetration testing of different network topologies are reviewed.

3.1. Wireless Local Area Network Penetration Testing

We live in an age of digital transformation that relies on wires and wireless networks to communicate and share information between devices. Network-based technology has become an integral part of government and private organizations to organize simple operations in different fields such as education, healthcare, purchasing, sales, manufacturing, and other areas. In addition, this technology is an integral part of individuals' daily lives, such as using social media, which depends on a network. This leads to interactivity and efficiency at work, but also poses many risks when attackers target the networks. The security attacks carried out by the attackers create a large amount of damage that can lead to the complete or partial destruction of the network infrastructure, which brings the work of organizations to a halt and causes financial losses that can go as far as bankruptcy. Wireless networks, also called WLANs, are one of the most popular types of networks today. Wireless networks have the advantage over current wired technologies in that they are convenient. As a result, attackers can target these networks, and this is why security issues are considered one of the most important and significant problems with wireless networks. Therefore, authentication protocols have been developed to prevent unauthorized access to wireless networks. There are two different types of wireless networks: wired equivalent privacy (WEP) and Wi-Fi protected access (WPA), and these are the most common encryption technologies. There are vulnerabilities in the WPA2 protocol that secures all modern protected Wi-Fi networks. According to Rajawat, G. et al. [13], there are vulnerabilities in the WPA2 protocol that secures all modern protected Wi-Fi networks. Attackers have attempted to exploit these vulnerabilities using key recovery attacks (KRACKs) to read information that was previously thought to be securely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, etc. To mitigate this threat, security plans must be in place to prevent, detect, and respond to it. One way to mitigate security risks in infrastructure is through network penetration testing. The concept of network penetration testing is very important because it performs the defence-in-depth process and takes preventive measures to protect networks from intruders. Therefore, network penetration testers must think the same way as criminals and perform the same tasks to close the vulnerabilities. Jain, S. et al. [14] performed penetration tests in IEEE 802.11 encryption protocols that define WLAN properties. They used various tools and technologies to perform attacks on IEEE 802.11 encryption protocols. These tools and technologies are Wi-Fi adapters, Raspberry Pi kit, Wi-Fi routers, Raspberry Pi (power adapter), Bluetooth adapters, Kali Linux, Aircrack-ng, Airodump-ng, and Airplay-ng. They performed attacks on WEP by intercepting all packets from the target access point (AP) and cracked the WEP key. On WEP2, they performed passphrase cracking from the recorded four-way handshake and KRACK attack, and on WEP3, they performed a downgrade attack. Agrawal, A. et al. [15] designed and implemented a system called CheckShake to passively detect anomalies in the handshake of Wi-Fi security protocols, particularly WPA2, including KRACK attacks. This system works without decrypting traffic and aims to develop a fully automated tool to detect KRACK attacks. They found that CheckShake can achieve an accuracy of 93.39% and a false positive rate of 5.08%. By formally modeling and evaluating the pre-authentication phase in accordance with the IEEE 802.11-2020 roll up, Hoque, N. et al. [16] have addressed one of the gaps in the formal analysis of the Wi-Fi protocol. This will enable them to prevent future large-scale security breaches such as KRACK attacks.

Table 4 illustrates the results of previous studies on WLAN penetration testing.

Table 4. Wireless local area network penetration testing.

Author	Publication	Vulnerability	Tools and System Used	Possible Attack
Rajawat, G. et al. [13]	2022	Vulnerabilities in the WPA2 protocol	Not mentioned	(KRACKs) Key recovery attack
Jain, S. et al. [14]	2020	Vulnerabilities in the IEEE 802.11 encryption protocol, WEP2, WEP3	Wi-Fi adapter—Raspberry Pi kit—Wi-Fi router—Raspberry Pi (power adapter)—Bluetooth adapter—Kali Linux—Aircrack-ng, Airodump-ng, Airplay-ng	KRACK attack, Downgrade attack
Agrawal, A. et al. [15]	2022	WAP2 protocol	CheckShake system.	KRACK attack
Hoque, N. et al. [16]	2022	Wi-Fi protocol	Optional OCV mechanism.	KRACK attack

3.2. Wireless Local Area Network Penetration Testing Architecture

The researchers proposed different architectural environments for the penetration testing of the wireless local area networks. The basic architecture is shown in Figure 2.

To begin the WLAN penetration testing, it is important to set up the environment. The components of the environment used in penetration testing are hardware and software [17]. The hardware components are routers, attacker devices such as laptops, WLAN cards, and approved clients such as mobile devices. The use of software tools such as "airodump-ng" and "aircrack-ng" to eavesdrop, sniff, and capture WLAN traffic is permitted. In addition, the AP and the allowed clients are forgeable with utilities "mac-changer" and "aireplay-ng". On the laptop used by the attacker to perform the attack and running Kali Linux as a penetration test OS, all software components are downloaded and installed. The client device (mobile) knows all of the clues about the target network. The client device is set up with a specific OS. The client device uses an AP to connect to the internet [17].

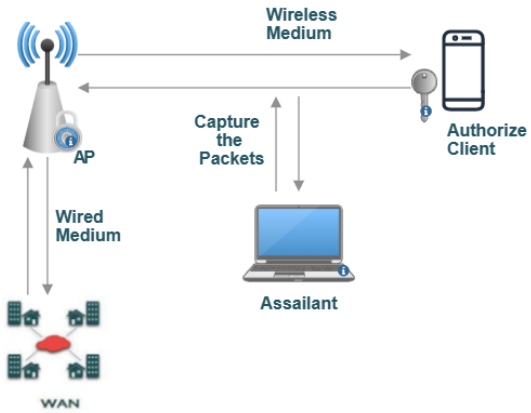

Figure 2. WLAN penetration testing architecture.

3.3. WLAN Penetration Testing Methodology

There are many types of standard methodologies that can be used in order to perform different types of network penetration tests. For WLAN penetration testing, the researchers present how to conduct penetration testing in a WLAN environment.

3.3.1. Reconnaissance/Gathering Information

In this phase, testers gather information about the network and its connections, search for information about the attack object, or create a footprint in a specific area without being detected. In addition, the testers determine the existing protection mechanisms in the target

system [18]. In addition, it is important to obtain information about the DHCP, DNS, and sub-net IP address.

3.3.2. Network Scanning

In this phase, security vulnerabilities in remote target networks or local hosts are identified. For this purpose, IP address information is collected from live hosts and Layer 2 devices. Then, the target hosts are scanned for open ports using tools such as Nmap and Nessus. In this way, tables of hosts with IP addresses and their corresponding MAC addresses are created along with open ports.

3.3.3. Exploitation

This technique is used to inject various forms of attacks into the network. Attack techniques to break into WLANs. The tests are performed using tools such as cracking attack tests, DoS, and password routers.

3.3.4. Post Exploitation

In this stage, consultations are conducted to provide advice on how to defend the target network. The methods described in this step are intended to help testers identify and document sensitive information, configuration settings, communication channels, and relationships with other network devices that can be used to further access the network. Network Penetration Testing Methodology is shown in Figure 3.

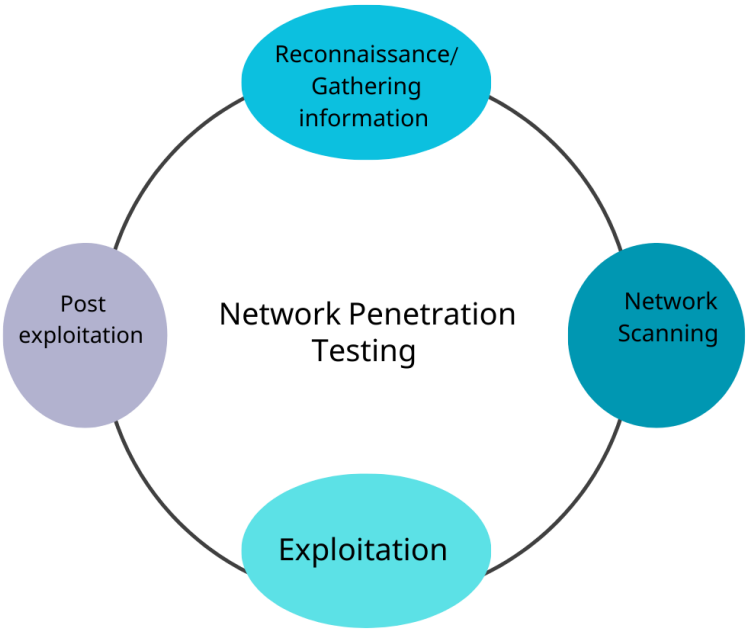

Figure 3. Network penetration testing.

3.4. Detecting Open Ports and Possible Attacks

The purpose of the study by Adamovi et al. [1] was to provide an overview of penetration testing for the novice penetration tester. In this way, the tester could identify the security vulnerability and make perfect recommendations to improve security and maintain the system. It was outlined that penetration testing has five phases, namely reconnaissance, scanning, gaining access, access maintenance, and report generation. It was also outlined that the methods of penetration testing are external testing, internal testing, blind testing, double blind testing, and targeted testing. Finally, some tools for penetration testing, such as Nmap, Shadow, Brup Suite, Metaspoilt, and Wireshark, were presented in detail.

The purpose of the study by Shah, M. et al. [3] was to propose a scanning strategy using the Nmap tool. This strategy illustrated how penetration testing deals with large sets of hosts. Initially, an IP table was used to monitor traffic sent to a given host before

1000 TCP popular ports were scanned on a host using Nmap tools. Then, network sweeping techniques were used, i.e., Nmap network sweeping scan with the -sn parameter, which used ICMP packets to scan hosts in the network. In addition, five timing options were used to control the scan time. The result showed that the fifth option required less scan time. This means that it needs to discover additional ports and services by using a more comprehensive scan and performing port scans blindly to open ports that make the security assessment more effective.

The purpose of the study by G. Jayasuryapal et al. [4] was to provide an overview of network penetration testing. The study illustrated all of the mechanisms of network penetration testing, including information gathering and subsequent exploitation. It also discussed the methodology of network penetration testing, which is divided into five steps. Prior to conducting a network penetration test, the tester must connect to the network LAN and perform an ARP ping scan to bypass the policy list and find the IP address. The test begins by collecting information such as the address of internal network sources (i.e., the IP address using the Google database, social media, and the company website). Then, in the scanning phase, tools, such as Nmap and Nessus, are used to find the hosts, ports, and running services to detect vulnerabilities. This is followed by enumeration and post-exploitation, and finally reporting. The study recommended performing network penetration tests to protect the company's IT data.

The purpose of the study by Khera, Y. et al. [6] was to protect against various cyber attacks. The paper illustrated the vulnerability assessment and penetration testing (VAPT) of the life cycle. It starts in the area where an attacker tries to obtain information about the victim, i.e., the victim's operating system. Then, the reconnaissance phase begins, and the security auditor gathers all of the information about the device or system. This data helps the security tester to plan the attack methods for the system. Then, in the vulnerability detection phase, the tester tries to find vulnerabilities in the system/device. In the information analysis and planning phase, the tester analyzes the risk identified during scanning to determine the cause and effect of the risk that will occur after the victim is exploited. The penetration phase (exploiting) focuses on external real risks. Privilege escalation is performed after penetration to identify and gain higher privileges. In the results analysis phase, recommendations are planned to address the risk or defect. Finally, in the reporting and clean-up phase, a report is created and executed to remove the temporary files and restore the system to its original state. This paper also introduced the network security assessment tools such as Wire Shark, Nmap, Metasploit, and Air Crack. It discussed that with the technique of VAPT, a user can discover the vulnerabilities that can lead to a variety of malicious attacks such as a denial-of-service DoS attack. Finally, the Nmap tool was implemented to track the activities of attackers and victims. It recommended performing a lot of security and pentesting, as the number of cyber attacks is increasing with the growing use of digital payments and the storage of digital data.

The purpose of the study by Al Shebli, H. et al. [10] was to focus on discussing the factors and components to be considered when performing penetration tests. The study contained an analysis of the methods used and the function of penetration testing in the implementation of IT governance in an organization. The methods based on the available information were black box, white box, and gray box. Penetration testing strategies were presented: external penetration, internal penetration, router penetration, firewall penetration, application penetration, password cracking penetration, and social engineering penetration. There were three phases for performing penetration testing at different levels of organizations and business units, namely test preparation, test execution, and test analysis. The main tools were discussed, namely Nmap, BeEF, Metasploit, Nessus, and Cain and Abel. Finally, penetration testing was discussed in IT security standards such as ISO 27000 as well as the ethics that the penetration testing team must possess. ISO standards used an information security management system based on the PDCA model, also known as the plan-do-check -act model, for penetration testing.

The purpose of the study by Cadiente, K. et al. [19] was to implement the vulnerability management process by applying a vulnerability assessment and penetration test (VAPT), to fix the vulnerabilities found in the network and to create an improved version of the network. In addition, it proposed to create 12 servers and a firewall by installing their respective OS images in the hypervisor. In the vulnerability assessment phase, the OpenVAS application used the Greenbone community feed to run the Linux environment. Then, Kali Linux was installed in the testing phase to use Metasploit for attack penetration. In this paper, it is suggested to install Fail2Ban to prevent brute force attacks via SSH. It also suggested updating the firewall by creating additional firewall policies. Upon applying the suggested measures, the vulnerabilities decreased compared to the results before implementing the suggestions. Finally, it suggested using manage switches to monitor and control the network LAN and prevent active threats. The paper recommended using other security configurations with Manage switches to protect the network.

The purpose of the study by P. Shi et al. [20] was to introduce a penetration testing framework for large networks based on network fingerprinting to address the limitations of traditional penetration testing in large networks. Two techniques were discussed, namely network fingerprinting and cyberspace search engine. There are two categories of fingerprint identification methods, namely active and passive. The active fingerprint requires tools to actively scan the network system for information, while the passive fingerprint passively listens to the network to obtain information. The proposed system architecture included the target acquisition module, the data processing module, and the test module. Finally, the advantages of using the proposed framework were discussed such as saving testing resources and limiting the risk of missing information.

The purpose of the study by A. M. Patel and H. R. Patel [21] was to provide an overview of penetration testing for wireless infrastructure security. Vulnerabilities put an organization's sensitive data at risk of attack, such as a poor framework and human error. It illustrated the type of penetration test, namely social engineering test, web application test, physical penetration test, network services test, client-side test, remote dial-up war dial, and wireless security test. It also presented the process of penetration testing and the criteria for selecting the best open source tools such as Nmap, Metasploit, Wireshar, OpenSSL, Cain and Abel, THC Hydra, and w3af to improve the security of the infrastructure. The study provided a diagram of the input testing procedure and the devices used.

B. Iyamuremye and H. Shima [22] focused on how SMEs can overcome the difficulties and enormous costs associated with testing networks in Rwanda. The study discussed the problems faced by SMEs such as the lack of network security experts and unknown network assets. The study suggested the use of user-friendly network security tools such as Nessus, Qualys, Nmap, and LAC Falcon. The proposed solution, SMEsec, included a sensor consisting of tools such as Nmap and a DoS attack simulator, database, filter, web portal, and a team of network security experts. SMEsec performed various tasks such as asset discovery, asset registry creation, vulnerability identification, and simulation of DoS attacks against the web server. The results showed that it is possible to improve SMEsec's network security status.

D. Overstreet et al. [23] tested the vulnerability of an Amazon Echo to a denial-of-service (DoS) attack. In this study, one instance of Kali Linux was used to perform the attacks on the device, while another instance of Kali was used to monitor the network during the attack. In this study, information was collected using the Nmap scan and the SPARTA tool in Kali Linux to obtain information about the open TCP ports on the device. Then, network traffic was analyzed using Wireshark to show where network packets were lost during the attack. This study revealed that it can be quite easy for an attacker with the knowledge and ability to gain access to a home network to obtain information about the connected devices using free and relatively simple penetration tools in Kali Linux. In the future, authors will perform more invasive penetration techniques.

U. Nisa and K. Kifayat [24] targeted TCP network traffic to detect the slow port scanning attacks. The study proposed an approach to detect slow port scanning attacks not

only over a static time interval, but also over all attacks that occur with a gradual increase or decrease in time duration. The proposed approach contained four modules: data acquisition, packet detection, scanning filter, and detection filter. The approach detected attacks using live data. It classified the single and parallel port scans based on the attempts made. This achieved discrimination between the faster and slower scans. This solution can be used to detect automatically scanning worms on the internet.

G. Bagyalakshmi et al. [25] discussed the analysis of network vulnerabilities in brain signal processing, which is important in healthcare. The study discussed that network device components, such as switches and routers, are vulnerable to various types of attacks such as viruses, worms, DoS, and Trojans. In addition, the attackers can inject malware or send their segments through IP spoofing and TCP session theft. The authors used different scanning techniques, such as ping sweep, TCP sweep, and null sweep, for the popular brain signal databases using Wireshark and Nmap tools. They found the ping sweep support status, TCP sweep times, and null scan times on different servers.

Rosihan and Muin, Y. [26] proposed to perform MikroTik router vulnerability testing for a network vulnerability evaluation with the penetration testing method. Their goal was to prevent possible threats such as DDoS attacks and brute force. They mentioned that DoS attacks were very common in 2021. The method used in this research is an experimental method. Thus, brute force and DDoS penetration tests were performed directly on the object. The tools used were Nmap for scanning and Routerploit.

Table 5 illustrates the results of previous studies on open ports and possible attacks.

Table 5. Summary of the open ports and possible attacks.

Author	Publication	Tool Used	Open Ports	Possible Attacks
Cadiente, K. et al. [19]	2020	Metaspoilt	SSH port 22	Brute force
Shah, M. et al. [3]	2019	Nmap	TCP port 65535 UDP port 65535 HTTP port 80 FTP port 21 SMPT port 25	The scan was for controlling the time of scan.
Khera, Y. et al. [6]	2019	Wireshark Nmap Metaspoilt AirCrack	FTP port 21 SHH port 22	Brute force Generate random number of its OpenSSL library.
Adamovic et al. [1]	2019	Nmap Metaspoilt Shadow Burp Suite Wireshark	Scan large number of ports. FTP server.	DoS attack
Al Shebli, H.et al. [10]	2018	Nmap BeEF Metaspoilt	Not mentioned	DoS attack Privilege escalation
G. Jayasuryapal, et al. [4]	2021	Nmap Nessus—ZAP—SQLMAP—WPSCAN—WEBSEARCH-Acunetix—Net sparker—Burp Scanner—NTOSpider	Not mentioned	Not mentioned

Table 5. *Cont.*

Author	Publication	Tool Used	Open Ports	Possible Attacks
P. Shi et al. [20]	2019	Shadow	TCP and UDP port range 1–65535.	Not mentioned
A. M. Patel and H. R. Patel [21]	2019	Nmap Metaspoilt Wireshark OpenSSl	General open ports.	MITM attack sniffing.
B. Iyamuremye and H. Shima [22]	2018	Nessus Nmap	Not mentioned General open ports.	DoS attacks
D. Overstreetet et al. [23]	2019	Nmap SPARTA	TCP ports	DoS attack
M. U. Nisa and K. Kifayat [24]	2020	Not mentioned.	TCP ports UDP ports FTP port 21	Scanning attacks
G. Bagyalakshim et al. [25]	2018	Nmap Wireshark	TCP ports	DoS attack Viruses Worm Trojans
Rosihan and Muin, Y. [26]	2022	Nmap	FTP Port 21, Domain port 53, HTTP port80, and HTTPS port 443	Brute force and DDoS attacks

3.5. Network Penetration Testing Methodologies

The purpose of the Astrida, M. et al. [11] study was to test the network vulnerability in the wireless local area network (WLAN) at SMP XYZ. Therefore, the authors used the penetration testing execution standard (PTES) method to analyze the attacks on the network XYZ SMP. The authors used four types of tests. In the WPA2 cracking test, the authors found that the WPA2 key could be cracked. In addition, the result of the DoS test was that the client connection to the access point was very easy to break because only the MAC address and SSID of the access point were needed. The password router wireless cracking test result determined that the level of vulnerability was high because the access point only used the default password. Finally, the authors performed an isolation test for the access point and found that clients could attack the client. Then, the authors proposed solutions to address these gaps, namely using a unique and strong WPA2 key with at least 15 characters, sector antennas as wireless network antennas, a unique and strong password with at least 15 characters, and configuring an AP isolation at the access point.

Alsahlany, A. et al. [17] conducted WLAN penetration tests to evaluate the security strength of the hidden SSID, MAC filtering, and WAP2. They found that the real name of the hidden SSID could be easily discovered. They also found that the MAC filter was not a major obstacle for the attackers and that WPA2 was a vulnerability to brute force attacks and human social factors. They recommended disabling the WPS protocol to prevent an attacker from exploiting the vulnerabilities of this protocol and discovering the default PIN. In addition, they recommended using more complex WPA2 passphrases.

Fikriyadi et al. [27] conducted WLAN penetration tests to assess the WLAN security. The assessment methods were the planning phase, the detection phase, the attack phase, and the reporting phase. In the planning phase, the authors identified all possible vulnerabilities in network resources that attackers could exploit and conduct attacks. This phase enabled the testers to take appropriate security measures to protect the network assistants. In addition, in the reconnaissance phase, the authors collected data by scanning the WLAN to identify the WLAN and the target of the access point attacks. In the attack

phase, the authors used Kali Linux with the Wireshark application to crack the encryption, bypass the address MAC, attack the infrastructure, and run MITM. The result showed that for the WLAN connection, when the attackers accessed the same internet service, it was not able to provide a secure connection to the end users from the infrastructure and man-in-the-middle attacks. When cracking the encryption, the attack on the RADIUS server failed to authenticate through the captive portal. Finally, the test to bypass the MAC address was successful because the MAC addresses could be changed virtually with the Mac Address Changer tool.

The purpose of the Wahyudi, E. et al. [28] study was to compare two RADIUS server security systems with a captive portal using OpenWRT in order to provide a secure alternative to high-performance WLANs and WPA2-PSK, to prevent unauthorized use of the internet. The captive portal system is an authentication and data security technique. For comparison, the authors utilized a wireless penetration test method. The method began with gathering information, creating threat models, capturing passwords, and generating reports. The authors found that the captive portal system was 80 percent more secure than WPA2-PSK. Thus, the captive portal system is very difficult to break down.

Syed, S. et al. [18] intended to determine the security level of Mehran University of Engineering and Technology's (MUET) campus area network, IP cameras, bio-metric systems, and switches deployed in the network. Therefore, they conducted a live network penetration test starting with reconnaissance, scanning, exploitation, and post-explosion. The authors proposed solutions to combat the threat such as changing the default credentials for all protocols configured in the network. In addition, remote access by unauthorized persons should be prevented. Finally, it was determined that restricted access and IDS or ARP inspection would prevent an ARP attack.

Kumar, R et al. [29] performed penetration testing in the network lab by demonstrating attacks and penetration of the network infrastructure. In addition, they used Kali Linux to perform penetration testing. The network penetration testing methodology included the phases of information gathering, vulnerability analysis, exploitation, and reporting. The authors used Dmitry, Nmap, and zenmap tools to gather information. In the second phase, the authors used Nexpose Community, Nessus, GFI Languard, and OpenVAS. In the exploration phase, they used Armitage and Metasploit framework to simulate possible attacks. Table 6 illustrates the results of previous studies on network penetration testing methodologies.

Table 6. Network penetration testing methodologies.

Author	Publication	Type of Network	Address Threats	Penetration Testing Techniques	Limitation
Fikriyadi et al. [27]	2020	WLAN	The WLAN is vulnerable to man-in-the-middle attacks, cracking the encryption, and sniffing packet.	The assessment methods were the planning phase, the detection phase, the attack phase, and the reporting phase.	The authors did not discuss enough about the tools and how to choose the best one.
Wahyudi, E. et al. [28]	2019	Wireless	In wireless networks, there are problems such as password theft, illegal access, and man-in-the-middle attacks.	The proposed methodology was gathering information, creating threat models, capturing passwords, and generating reports.	The result showed that it is very difficult to crack the system using ARP attack techniques, spoofing, brute force, and sniffing for eavesdropping, so the authors must adapt other network traffic sniffing tools to detect other types of network vulnerabilities.

Table 6. *Cont.*

Author	Publication	Type of Network	Address Threats	Penetration Testing Techniques	Limitation
Astrida, M. et al. [11]	2022	WLAN at SMP XYZ	There are vulnerabilities related to cracking WPA2, DoS, cracking wireless router passwords, and isolating access points.	The authors used the penetration testing execution standard (PTES). The stages of the PTES are: pre-engagement, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. In addition the authors performed four types of attack tests and found a solution to fix the gaps.	There are no limitations.
Syed, S. et al. [18]	2020	Campus Area Network	There are vulnerabilities in the operating system.	The authors used gray hat penetration testing. The phases were reconnaissance information collection, network scanning, exploitation, and post-exploitation.	The results were not clear enough and there is no future view.
Alsahlany, A. et al. [17]	2018	WLAN	The WPA II is vulnerable to brute force attacks and human social factors.	The authors conducted WLAN penetration testing in the following phases: reconnaissance, scanning, exploitation, and post exploitation.	The tests showed that the WPS protocol must be turned off and the passphrases changed regularly to prevent potential attackers from exploiting the vulnerabilities. Finally, the penetration tests showed that the security measures are in place but need to be improved and used more effectively.
Kumar, R. et al. [9]	2018	Internal Network	The host was vulnerable to buffer overflow, spoofing, remote code execution, denial-of-service, and privilege escalation.	The proposed methodology for penetration testing are planning, vulnerability discovery, attack and reporting.	There are no limitations.

3.6. Techniques for Protecting Open Ports against Vulnerabilities

The purpose of the study by Pandey et al. [30] was to propose the use of the Raspberry Pi 3b+ (portable minicomputer) in performing penetration testing to identify vulnerabilities in the network using assessment tools such as the integrated pentesting tool. The vulnerability assessment has three types, which are host-based, network-based, and database-based. In addition, the process of penetration testing was discussed, which consisted of reconnaissance, scanning, gaining access, maintaining access, and analysis. It also discussed how vulnerability assessment and penetration testing (VAPT) help assess and protect the system. There are advantages to using a single board to perform VAPT. This study will be helpful in developing portable devices in new and innovative ways to improve and strengthen cyber security.

Liao et al. [31] suggested finding an efficient way to detect Nmap scanning behavior because the intrusion detection system (IDS) is used to protect hosts from malicious intrusion. The authors proposed comprehensive Nmap detection rules (CNDR). In CNDR, Nmap's customizable fields were removed and rules for scanning the operating system were added. CNDR achieved 100 percent detection rate for normal Nmap scans and 91.7 percent detection accuracy for Nmap with IDS evasion on the researchers' designed database.

Ernawati, T. et al. [32] conducted three types of attacks: port scanning, DDoS SYN flood, and brute force attack to analyze the performance of IDS (PSAD, Portsentry and Suricata) with certain parameters, namely detection speed, detection accuracy, and resource consumption. The authors found that the accuracy of the detection parameters was 100 percent for all three attacks. Suricata and PSAD have better performance when used as a network IDS. Portsentry cannot defend against brute force attacks, but it can defend against port scanning attacks and prevent denial-of-service attacks. The authors hope to test more new parameters in the future.

Kumar et al. [9] proposed a system for detecting, fixing, and reporting security vulnerabilities in local area networks to prevent attacks. The system is primarily intended for Linux/Windows network administrators. It was also developed in Python and is supported by Kali Linux. The authors discussed that there are many tools that can be used to find logically open ports, such as Sparta, OpenVAS, Nessus, and Nmap, but there are no tools used for physically open ports. The proposed tool, the fixing network security vulnerability tool (FNSV), can scan and secure physically open ports using a series of Telnet and SSH commands. In addition, it can scan various vulnerabilities in a network, website, or system and scan a specific IP address or range of IP addresses. It can be used in various network scenarios.

Hartpence, Bruce, and Andres Kwasinski [33] discussed that port scans can be used as an attack and cause problems with application performance and productivity. The authors illustrated how sequential neural networks (NNs) are used to classify packets, separate TCP datagrams, identify the type of TCP packets, and detect port scans. The authors noted that NNs are flexible and can learn from different environments and partition complex tasks. This helps in protocol classification and achieves accuracy rates of over 99 percent. It is effective in detecting TCP port scan attacks.

Gupta, A., Sharma, L. S. [34] suggested using the intrusion detection and prevention system (IDPS) Snort to mitigate network attacks. The authors created Snort-IDS rules for various DoS and port scan attacks. The results showed that for a TCP reset, Xmas tree, UDP flood, SYN flood, DNS flood, ICMP flood, and Smurf attacks, the percentage of detected attack packets was 98 percent. In addition, for the ACK scan and null scan, the percentage of attack packets detected was 100 percent. In the future, the authors will introduce the Snort-IDS rules to detect other types of attacks.

Neu, Charles V. et al. [35] discussed a new port scanning system IPS for SDN based on OpenFlow switch counter data to prevent port scanning attacks. The authors first detected port scan flows and then updated the OpenFlow routing rules to ensure network security. This method was very effective at detecting malicious flows and had a low false negative rate. The system was lightweight and considered resource consumption such as network bandwidth and memory usage. For future work, the authors will use this technique to detect other attacks such as DoS.

Wu, Daoyuan et al. [36] discussed open ports in Android apps and their threats by opening a port analysis pipeline that included discovery, diagnosis, and security assessments. The study spanned a 10-month period. The researchers collected more than 40 million port monitoring records. In the discovery phase, they used crowdsourcing, which provided a more detailed view of the prevalence of open ports in Android apps. Then, in the diagnosis phase, they used static analysis to obtain more detailed information about the security impact of the open ports. Finally, they conducted security assessments of open ports, namely a vulnerability analysis in a denial-of-service attack assessment and inter-device connectivity measurement. They proposed solutions to mitigate the open port attack in Android. They are app developers, SDK vendors, system vendors, and network operators.

The study by Luswata, John, et al. [37] aimed to provide an overview of attacks on SCADA (supervisory control and data acquisition) systems, focusing on systems that use Modbus TCP. To do this, the authors conducted penetration tests using the smod tool to identify common vulnerabilities, examined internal and external attacks, and studied

the efficiency and effectiveness of the new tool. They also discussed testing capabilities for information security availability (denial-of-service) and integrity (address resolution protocol poisoning). IDS and the modbusfw firewall was used to defend against and detect a DoS attack. The results showed that some attacks affected integrity and availability. Finally, it was recommended to improve the security of the SCADA system.

The purpose of Shah, Nishit, and S. Shravan's [38] study was mainly to investigate different web applications against DDoS attacks to determine the protection level of servers against DDoS attacks. The authors used the Slowloris tool for DDoS attacks in penetration testing to make many HTTP requests and attack the web server regularly. In addition, they used Wireshark to capture the packets. They discussed the common DDoS attacks, namely application level attacks (sending HTTP traffic load with malicious intent) and protocol attacks (TCP handshake). Using Python Sklearn for the random forest classifier, the authors found that the predicates were 99 percent accurate and matched the proposed model.

Chaudhary, S. et al. [39] advised automating penetration testing, especially the post-exploitation phase, to search the hijacked network and find critical data. They suggested using Q-learning to train the agent and create a suitable environment. To estimate the Q values in different network contexts, the method uses neural networks. Although the authors propose this, they have not yet put it into practice.

Hu, Zhenguo et al. [40] proposed the use of an automated penetration testing framework based on deep reinforcement learning (DQN) technology to offer potential tactics. To discover all potential attack routes and create the matrix representation required by deep reinforcement learning algorithms, the authors used conventional search algorithms. They then use the deep Q-learning network (DQN) approach to select the simplest attack route from a list of potential candidates. The shortcoming of this work was the lack of a network service scanning capability that would automatically feed the DQN model with data about the actual target environment.

Niculae, Stefan et al. [41] compared several algorithms for determining an attacker strategy, from fixed strategy to reinforcement learning, namely Q-learning (QL), extended classifier system (XCS), and deep Q network (DQN). The results were that QL was better than human performance, XCS was worse than human performance but was more stable. DQN did not achieve comparable performance. All of these machine learning approaches outperformed the fixed strategy attackers.

Ghanem, Mohamed C. et al. [42] proposed to make penetration testing smarter and more efficient by using reinforcement learning. Intelligent automated penetration testing framework is the name of the proposed model (IAPTF). It uses model-based reinforcement learning for automatic sequential decision making. To find the most effective decisions, it uses partially observed Markov decisions (POMDs). Results show that IAPTF with hierarchical network modeling outperforms traditional methods and human performance over time, with the advantage increasing with network size.

Erdődi, L. et al. [43] proposed to simulate an SQL injection vulnerability. They modeled it as a Markov decision process. Then, they implemented it as a reinforcement learning problem. The result showed that an agent with reinforcement learning can be used for penetration testing. This work had the drawback that the type of vulnerabilities could not be executed and the agent was only useful for certain challenges, but not for real cases.

Motghare, V. et al. [44] proposed a system that contained three security tools in software with a graphical user interface. The toolbox included a port scanner, a tool for encrypting and decrypting text, and a password cracker. The system aimed to save the researcher time and provide a hassle-free and easy way to use the tools to help with the search.

Table 7 illustrates the previous qualitative and quantitative researches. We compare the qualitative and quantitative research that has addressed the issues of vulnerability prevention and mitigation.

Table 7. Summary of the mitigation techniques for protecting open ports against vulnerabilities.

Author	Publication	Research Methodology	Mitigation Technique
R. Pandey et al. [30]	2020	Qualitative	Proposed using Raspberry Pi 3b+ and improved security by using VAPT
S. Liao et al. [31]	2020	Qualitative	Proposed comprehensive Nmap detection rules.
Ernawati, T.et al. [32]	2019	Qualitative	Improved security by conducting three types of attacks to analyze the performance of IDS
B. K. Kumar et al. [9]	2019	Qualitative	Proposed system for detecting, fixing and reporting security vulnerabilities in networks to prevent attacks.
B. Hartpence and A. Kwasinski [33]	2020	Qualitative	Suggested to use sequential neural networks to detect port scans.
Gupta, A. and Sharma, L. S [34]	2019	Qualitative	Suggested to use intrusion detection and prevention system snort for various Dos and port scan attacks.
C. V. Neu et al. [35]	2018	Qualitative	Proposed using a new port scanning system IPS for SDN to prevent port scanning attacks such as DoS attack.
WU daoyuan et al. [36]	2019	Qualitative	Proposed the first analysis pipeline covering open port detection, diagnosis, and security assessment.
J. Luswata et al. [37]	2018	Qualitative	Used IDS and modbusfw firewall to defend against DoS attack in SCADA system.
G.Bagyalakshim et al. [25]	2021	Qualitative	Proposed model to investigate different against DDoS attacks to determine the level of protection. They found the proposed model was accurate.
Chaudhary. S.et al. [39]	2020	Qualitative	Proposed automated Post-Breach Penetration Testing through Reinforcement Learning
Hu, Zhenguo et al. [40]	2020	Qualitative	proposed to use an automated penetration testing framework based on Deep Reinforecment Learning (DQN) technique
Niculae, Stefan et al. [41]	2020	Qualitative	Comparison of multiple machine learning algorithms to select the best algorithm for penetration testing.
Ghanem, Mohamed C.et al. [42]	2022	Qualitative	Proposed (IAPTF) with Markov decision to determine the best efficient option in penetration testing.
Erdődi.L.et al. [43]	2021	Qualitative	Performed penetration testing by modeling SQL injection. Modeled using Markov decision processes and agents with reinforcement learning.
Motghare.V. et al. [44]	2022	Qualitative	They proposed a software that includes a toolbox to save time and find the vulnerabilities easily and quickly.

4. Results and Discussion

In this section, the results of the analysis of the previous studies are presented.

4.1. Wireless Local Area Network Penetration testing

According to the studies analyzed, the vulnerabilities in the WLAN were vulnerabilities in the IEEE 802.11 encryption protocol, namely WEP2 and WEP3. The possible attacks were the KRACK attack and Downgrade attack.

4.2. Tools to Detect Open Ports

According to the studies analyzed, the common scanning tools used to detect vulnerable ports are Nmap, Metaspoilt, Wireshark, shadow, Nessus, AirCrack, Brup suit, BeEF, SPARTA, etc. As shown in Figure 4, the most commonly suggested tool is Nmap.

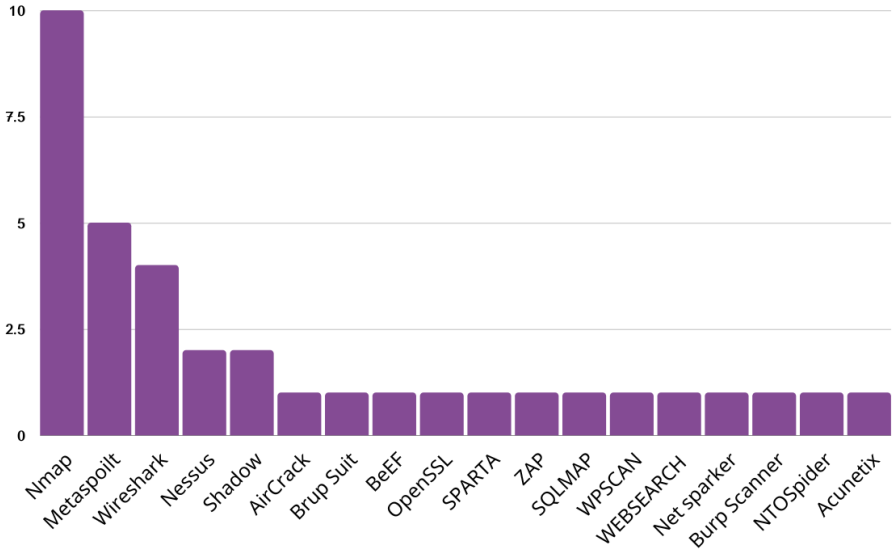

Figure 4. Common Tools to Detect Open Ports.

4.3. Open Ports

Many ports have known vulnerabilities that you can exploit if they show up in the scanning phase of penetration testing. Here are the open ports shown in previous studies and that have been exploited.Transmission control protocol (TCP), which is the most common network protocol, and file transfer protocol (FTP) have been mentioned in previous studies. Figure 5 illustrates the most common open ports.

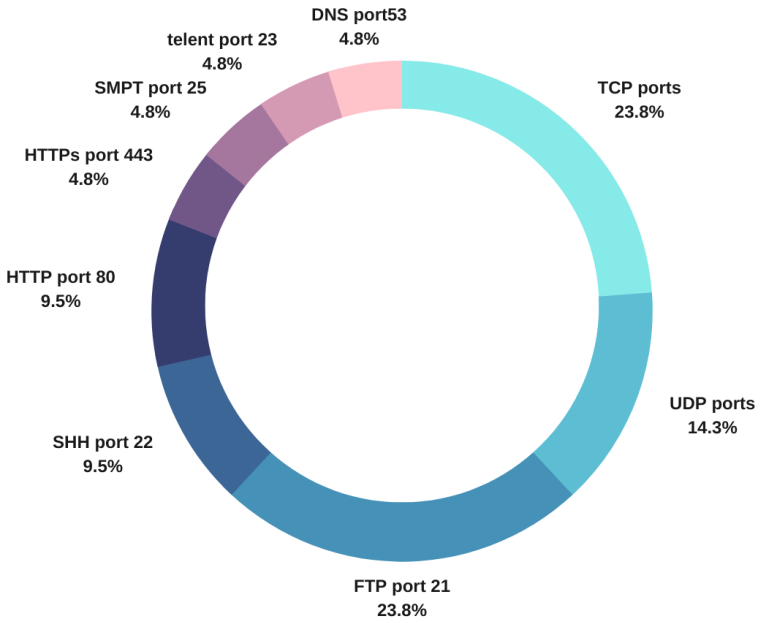

Figure 5. Open ports.

4.4. Network Penetration Testing Methodologies

According to our findings, there are many methods for network penetration testing, but they all have the same idea, which is to collect information about the target network, scan it, detect the vulnerabilities, perform attacks, and then provide remediation actions and recommendations in the reports.

4.5. Types of Attacks Exploiting Open Ports

The previous studies have shown that there are many types of attacks on vulnerable ports, and this is a security risk. These exploit system deficiencies to gain access to assets with the intent to cause harm. In 13 studies, the network layer threats that exploited the open ports were: DoS attacks, brute force, MITM, Open SSL library random number generation, sniffing, viruses, worms, Trojans, etc. The weak topology of the network leads to very simple attacks with all types of attacks (See Figure 6).

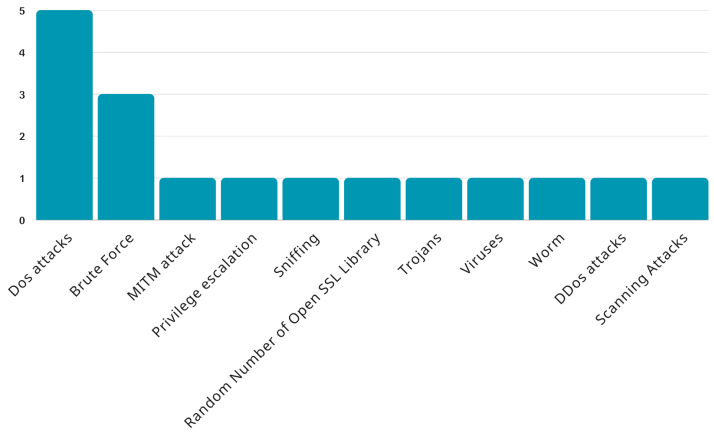

Figure 6. Types of attacks.

4.6. Mitigation Techniques for Protecting Open Ports against Vulnerabilities

The most common techniques for detecting and protecting open ports and saving time, according to the studies analyzed, are machine learning, VAPT, DOPA, Nmap detection rules, fixing network vulnerability tool (FNSV), and creating software for penetration testing with a toolbox. As Figure 7 shows, the most commonly proposed technique is machine learning.

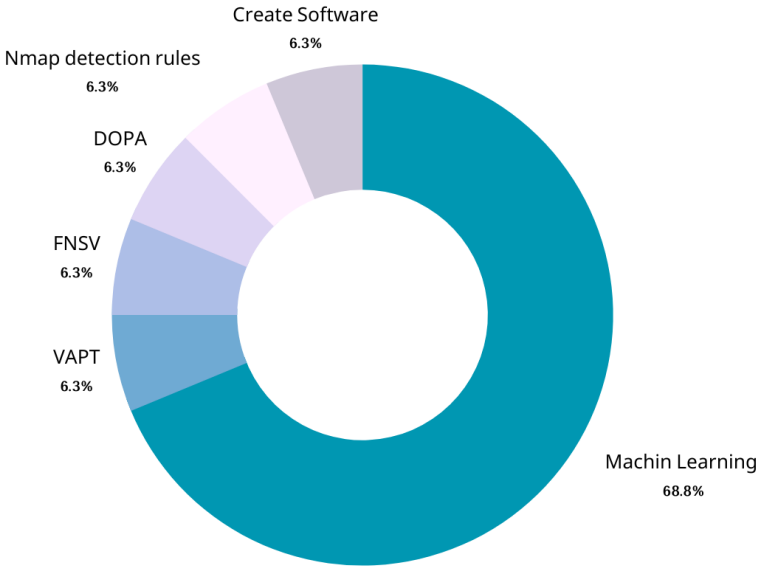

Figure 7. Techniques for Protecting Open Ports

5. Recommendations for Future Research Directions

We live in a time of developing technologies that depend on information systems for important operations, management and sharing of information. Many researchers are concerned about the security of these technologies before the risk occurs. Thus, we find that cyber security teams are focusing on penetration testing. In our paper, we provided

an overview of network penetration testing techniques. In this study, we summarize the following future directions:

First, we recommend further research on the use of machine learning with deep reinforcement learning to improve network penetration testing with specific topology of network which is WLAN network.

Second, although there is a lot of researches on network penetration testing, many types of attacks are still not considered and simulated in network penetration testing, specifically real attacks such as KRACKS attacks.

Third, one of the main concerns in network penetration testing is to detect most of the vulnerabilities in the technology before they are exploited, and the probability of false detection should be low.

The researchers [6] illustrated that manual network penetration testing is complex, competent penetration testers are not widely available, and the manual process is time-consuming and costly. Manual network penetration testing cannot achieve the speed and frequency required for efficient, large-scale development of security solutions. A team of experts can come together to develop a professional automated tool that is a combination of the experiences of the experienced penetration testers, so that the non-expert users can replace the penetration team with the automated tools based on machine learning to get a comprehensive overview of the security situation in the company's system. Therefore, we need more research investigating the deployment of automated penetration testing based on deep reinforcement learning to address these challenges.

6. Conclusions

In this study, a systematic literature review of 39 existing research publications on network penetration testing was conducted. This study provided a comprehensive review of 39 studies that address network penetration testing and open ports that need to be considered to prevent attacks. It also analyzed the most common types of attacks simulated during penetration testing and the techniques used to protect open ports from vulnerabilities. According to the results, the Nmap tool is the most common tool for network penetration testing, and DoS attacks were a common threat to open ports. Rosihan and Muin mentioned that DoS attacks are very common attacks [26]. In addition, the study found that the most commonly suggested remediation technique for vulnerable ports is using deep reinforcement learning. However, few studies have discussed that network penetration testing has certain limitations. Therefore, In future, we will focus on automated network penetration testing based on deep reinforcement learning with specific topology, which is the WLAN in order to identify real attacks such as KRACK Attacks.

Author Contributions: Conceptualization, M.A. and M.M.H.R.; methodology, M.A. and M.M.H.R.; software, M.A. and M.M.H.R.; validation, M.A. and M.M.H.R.; formal analysis, M.A.; investigation, M.M.H.R. and M.A.; resources, M.A. and M.M.H.R.; writing original draft preparation, M.A.; writing review and editing, M.M.H.R.; supervision, M.M.H.R.; project administration, M.M.H.R.; funding acquisition, M.M.H.R. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was funded by King Faisal University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. 3472]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which improved the quality and clarity of the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Adamovi, S. Penetration testing and vulnerability assessment: introduction, phases, tools and methods. In *Sinteza 2019-International Scientific Conference on Information Technology and Data Related Research*; Singidunum University: Belgrade, Serbia, 2019; pp. 229–234
2. Tidy, J. Swedish Coop Supermarkets Shut Due to Us Ransomware Cyber-Attack. *BBC News*, 3 July 2021. Available online: https://www.bbc.com/news/technology-57707530 (accessed on 17 May 2023).
3. Shah, M.; Ahmed, S.; Saeed, K.; Junaid, M.; Khan, H. Penetration testing active reconnaissance phase–optimized port scanning with nmap tool. In Proceedings of the IEEE 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 30–31 January 2019; pp. 1–6.
4. Jayasuryapal, G.; Meher Pranay, P.; Kaur, H. A Survey on Network Penetration Testing. In Proceedings of the IEEE 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 28–30 April 2021.
5. Packetlabs. Black-Box vs. Grey-Box vs. White-Box Penetration Testing. 19 April 2022. Available online: https://www.packetlabs.net/posts/types-of-penetration-testing/ (accessed on 6 May 2023).
6. Khera, Y.; Kumar, D.; Garg, N. Analysis and Impact of Vulnerability Assessment and Penetration Testing. In Proceedings of the IEEE 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 14–16 February 2019.
7. Press, T.A. T-Mobile Says Breach Exposed Personal Data of 37 Million Customers. *NPR*, 20 January 2023. Available online: https://www.npr.org/2023/01/20/1150215382/t-mobile-data-37-million-customers-stolen (accessed on 12 May 2023).
8. Farah, A.-D.; Alshammari, E. Automated penetration testing: An overview. In Proceedings of the 4th International Conference on Natural Language Computing, Copenhagen, Denmark, 31 October–4 November 2018.
9. Kumar, B.K.; Raj, N.; Dhivvya, J.P.; Muralidharan, D. Fixing Network Security Vulnerabilities in Local Area Network. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1349–1354.
10. Shebli, A.; Mohammed Zaher, H.; Beheshti, B.D. A study on penetration testing process and tools. In Proceedings of the 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 4–8 May 2018.
11. Astrida, D.N.; Saputra, A.R.; Assaufi, A.I. Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES). *Sink. J. Dan Penelit. Tek. Inform.* **2022**, *7*, 147–154. [CrossRef]
12. Singh, N.; Meherhomji, V.; Chandavarkar, B.R. Automated versus manual approach of web application penetration testing'. In Proceedings of the IEEE 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; pp. 1–6.
13. Singh, Rajawat, G.; Sharma, J. WIRELESS CYBERSPACE. *J. Anal. Comput. (JAC)*. **2022**, *16*, 1–4.
14. Jain, S.; Pruthi, S.; Yadav, V. Ethical Hacking of IEEE 802.11 Encryption Protocols. *J. Xi'an Shiyou Univ. Nat. Sci. Ed.* **2009**, *18*, 108–112.
15. Agrawal, A.; Chatterjee, U.; Maiti, R.R. CheckShake: Passively detecting anomaly in Wi-Fi security handshake using gradient boosting based ensemble learning. *IEEE Trans. Dependable Secur. Comput.* **2023**, 1–13. [CrossRef]
16. Hoque, N.; Rahbari, H.; Rezendes, C. Systematically Analyzing Vulnerabilities in the Connection Establishment Phase of Wi-Fi Systems. In Proceedings of the 2022 IEEE Conference on Communications and Network Security (CNS), Austin, TX, USA, 3–5 October 2022; pp. 64–72.
17. Alsahlany, A.M.; Alfatlawy, Z.H.; Almusawy, A.R. Experimental Evaluation of Different Penetration Security Levels in Wireless Local Area Network. *J. Commun.* **2018**, *13*, 723–729. [CrossRef]
18. Syed, S.; Khuhawar, F.; Arain, K.; Kaimkhani, T.; Syed, Z.; Sheikh, H.; Khan, S. *Case Study: Intranet Penetration Testing of MUET*; Mehran University of Engineering and Technology: Jamshoro, Pakistan, 2020; pp. 17–19
19. Cadiente, K.A.; Castro, R.A.; Gica, E.V.; Mora, K.M.; Ternio, J.V. Applying vulnerability assessment and penetration testing (vapt) and network enhancement on the network. *Infrastruct. Journey Tech Inc. Innov.* **2020**, *3*, 1.
20. Shi, P.; Qin, F.; Cheng, R.; Zhu, K. The penetration testing framework for large-scale network based on network fingerprint. In Proceedings of the IEEE 2019 International Conference on Communications, Information System and Computer Engineering (CISCE), Haikou, China, 5–7 July 2019.
21. Patel, A.M.; Patel, H.R. Analytical study of penetration testing for wireless infrastructure security. In Proceedings of the IEEE 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 21–23 March 2019.
22. Iyamuremye, B.; Hisato, S. Network security testing tools for SMEs (small and medium enterprises). In Proceedings of the IEEE 2018 International Conference on Applied System Invention (ICASI), Tokyo, Japan, 13–17 April 2018.
23. Overstreet, D.; Wimmer, H.; Haddad, R.J. Penetration Testing of the Amazon Echo Digital Voice Assistant Using a Denial-ofService Attack. In Proceedings of the IEEE 2019 SoutheastCon, Huntsville, AL, USA, 11–14 April 2019.
24. U Nisa, M.; Kashif, K. Detection of slow port scanning attacks. In Proceedings of the IEEE 2020 International Conference on Cyber Warfare and Security (ICCWS), Norfolk, VA, USA 12–13 March 2020.
25. Bagyalakshmi, G.; Rajkumar, G.; Arunkumar, N.; Easwaran, M.; Narasimhan, K.; Elamaran, V.; Solarte, M.; Hernández, I.; Ramirez-Gonzalez, G. Network vulnerability analysis on brain signal/image databases using Nmap and Wireshark tools. *IEEE Access* **2018**, *6*, 57144–57151. [CrossRef]

26. Muin, Y. MikroTik Router Vulnerability Testing for Network Vulnerability Evaluation using Penetration Testing Method. *Int. J. Comput. Appl.* **2022**, *975*, 8887.
27. Fikriyadi, F.; Ritzkal, R.; Prakosa, B.A. Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. *J. Mantik* **2020**, *4*, 1658–1662.
28. Wahyudi, E.; Luthfi, E.T.; Efendi, M.M.; Mataram, S.T. Wireless penetration testing method to analyze WPA2-PSK system security and captive portal. *J. Explor. Stmik Mataram* **2019**, *9*, 1. [CrossRef]
29. Kumar, R.; Katlego, T. Internal network penetration testing using free/open source tools: Network and system administration approach. In Proceedings of the International Conference on Advanced Informatics for Computing Research, Shimla, India, 14–15 July 2018; Springer: Singapore, 2018.
30. Pandey, R.; Vutukuru, J.; Chopra, U.K. Vulnerability assessment and penetration testing: A portable solution Implementation. In Proceedings of the IEEE 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 25–26 September 2020.
31. Liao, S.; Zhou, C.; Zhao, Y.; Zhang, Z.; Zhang, C.; Gao, Y.; Zhong, G. A Comprehensive detection approach of Nmap: Principles, rules and experiments. In Proceedings of the IEEE 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Chongqing, China, 29–30 October 2020.
32. Ernawati, T.; Fachrozi, M.F.; Syaputri, D.D. Analysis of Intrusion Detection System Performance for the Port Scan Attack Detector, Portsentry, and Suricata. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2019; Volume 662.
33. Hartpence, B.; Kwasinski, A. Combating TCP port scan attacks using sequential neural networks. In Proceedings of the IEEE 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 17–20 Feburary 2020.
34. Gupta, A.; Sharma, L.S. Mitigation of dos and port scan attacks using snort. *Int. J. Comput. Sci. Eng.* **2019**, *7*, 248–258. [CrossRef]
35. Neu, C.V.; Tatsch, C.G.; Lunardi, R.C.; Michelin, R.A.; Orozco, A.M.; Zorzo, A.F. Lightweight IPS for port scan in OpenFlow SDN networks. In Proceedings of the IEEE NOMS 2018—2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018.
36. Wu, D.; Gao, D.; Chang, R.K.; He, E.; Cheng, E.K.; Deng, R.H. Understanding open ports in Android applications: Discovery, diagnosis, and security assessment. In Proceedings of the Network and Distributed System Security Symposium 26th NDSS 2019, San Diego, CA, USA, 24–27 February 2019; p. 1.
37. Luswata, J.; Zavarsky, P.; Swar, B.; Zvabva, D. Analysis of scada security using penetration testing: A case study on modbus tcp protocol. In Proceedings of the IEEE 2018 29th Biennial Symposium on Communications (BSC), Toronto, ON, Canada, 6–7 June 2018.
38. Shah, N.; Shravan, S. Server Stress Test Using DDoS Attack. *Int. J. Res. Eng. Sci.* **2021**, *9*, 53–58.
39. Chaudhary, S.; O'Brien, A.; Xu, S. Automated post-breach penetration testing through reinforcement learning. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020.
40. Hu, Z.; Beuran, R.; Tan, Y. Automated penetration testing using deep reinforcement learning. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020.
41. Niculae, S.; Dichiu, D.; Yang, K.; Bäck, T. *Automating Penetration Testing Using Reinforcement Learning*; Experimental Research Unit Bitdefender: Bucharest, Romania, 2020.
42. Ghanem, M.C.; Chen, T.M.; Nepomuceno, E.G. Hierarchical reinforcement learning for efficient and effective automated penetration testing of large networks. *J. Intell. Inf. Syst.* **2022**, *60*, 281–303. [CrossRef]
43. Erdődi, L.; Sommervoll, ÅÅ; Zennaro, F.M. Simulating SQL injection vulnerability exploitation using Q-learning reinforcement learning agents. *J. Inf. Secur. Appl.* **2021**, *61*, 102903. [CrossRef]
44. Motghare, V.; Kasturi, A.; Kokare, A.; Sankhe, A. Securezy—A Penetration Testing Toolbox. *Int. Res. J. Eng. Technol.* **2022**, *9*, 2375–2378.