sustainability

MDPI

Review

Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods

Kamal Uddin Sarker *, Farizah Yunus and Aziz Deraman

Informatics, FTKKI, Universiti Malaysia Terengganu, Kuala Terengganu 21030, Malaysia; farizah.yunus@umt.edu.my (F.Y.); a.d@umt.edu.my (A.D.)

* Correspondence: ku-sarker@yahoo.com or kusarker@umt.edu.my; Tel.: +60-0163-331-474

Abstract: Cyber attackers are becoming smarter, and at the end of the day, many novel attacks are hosted in the cyber world. Security issues become more complex and critical when the number of services and subscribers increases due to advanced technologies. To ensure a secure environment, cyber professionals suggest reviewing the information security posture of the organization regularly via security experts, which is known as penetration testing. A pen tester executes a penetration test of an organization according to the frameworks and standardization guidelines. Security breaches of the system, loopholes in OS or applications, network vulnerabilities, and breaking data integration scopes are identified, and appropriate remediation is suggested by a pen tester team. The main aim of a penetration process is to fix the vulnerabilities prior to the attack in tangible and intangible resources. Firstly, this review work clarifies the penetration conception and is followed by the taxonomy of penetration domains, frameworks, standards, tools, and scoring methods. It performs a comparison study on the aforementioned items that develops guidelines for selecting an appropriate item set for the penetration process according to the demand of the organization. This paper ends with a constructive observation along with a discussion on recent penetration trends and the scope of future research.

Keywords: vulnerability; cybersecurity; penetration testing; quality of service; sustainability

Citation: Sarker, K.U.; Yunus, F.; Deraman, A. Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods. *Sustainability* **2023**, *15*, 10471. https://doi.org/10.3390/su151310471

Academic Editors: Kamal Bechkoum and Martin Wynn

Received: 30 April 2023
Revised: 11 June 2023
Accepted: 12 June 2023
Published: 3 July 2023

1. Introduction

The internet is becoming an essential space for all people to access public and private services, learning materials, social networking sites, communicating applications, and personal entertainment webpages. The services in the cyberspace are ingraining in every aspect of daily life [1]; as a result, we are generating a lot of private and sensitive information through online business [2], digital transactions [3], ecommerce [4], virtual learning platforms [5], telehealth [6], audio/video conferencing [7], reliable treatment [8], aviation and shipping services [9], mobile payment systems [10], etc. Cyber risk continuously rises at an alarming rate, compromising users' credentials, breaking data integrity, and stalling services, which is becoming one of the most important anxieties in the corporate world [1,11].

A cyberattack can ruin a victim's services, physical infrastructure, and logical connectivity by disrupting business continuity, damaging their reputation, or obtaining intellectual property [12]. Hackers can steal physical assets or secrete information [13] that can be used in religious propagation [14] or political agendas [11]. Sometimes, hacking happens for individual interests, such as for ransom money [14], showing hacking skills [14], or earning money by sharing information with a third party [15]. An attack causes economic losses [15] by deducting the number of customers [16], compromising reputations [12], adding extra expenditures for fixing [14,17], disturbing general growth [16,17], and increasing stakeholders' frustration or anxiety [18–20]. Moreover, a massive attack could be a reason for bankruptcy as well [21], and it is very crucial in military and national information mysteries in international policies.

The number of cybercriminals is increasing steeply with new attacking techniques [22], and they are becoming more cunning day by day [23]. New attacks and vulnerabilities are appearing every day, and organizations are updating new tools and techniques regularly to protect themselves. Purplesce [24] published a list of recent attacks on their website, including the largest DDoS attacks on Akamai, which were detected and protected by a victim in June 2022; the UNC2447 cybercrime gang with other groups compromised the credentials of Cisco employees in May 2022; Cloudflare noticed that they were under the threat in August 2022; Cleartrip detected a massive data breach in June 2022, etc.

Cyber criminals use loopholes that belong to devices, applications, networks, and users' activities to attempt an attack on a system. The design flaws of software and hardware, poorly configured systems or networks, obsolete hardware and software, complex computing systems, and human errors are common loopholes that are used by cybercriminals [1,11,12]. Government agencies, private organizations, and international trade centers show their attention to cyber defense [25]. A cyber defense is verified by penetration, which is a set of activities for examining physical and logical infrastructure along with the policy and procedures of an organization. It assesses and presents the vulnerabilities of an organization so that it can take remedial actions prior to a cyberattack. It is becoming a common and integrated part of an enterprise to review and update their systems regularly. An enterprise can execute a pen test for newly implemented information systems, after upgrading a system, or periodically (once nearly) [26,27]. Software product line vulnerability testing is also considered as a penetration test [28]. In general, penetration means a regular review practice that measures the security posture and reduces the risk of a cyber-attack [29,30].

Penetration frameworks support maximizing the scope of coverage and completing the reviewing process within a timeframe. This is the art of finding significant vulnerabilities that can cause attacks and minimize the possibility of security breaches. The penetration framework concentrated on the "security compliance testing", "staff's awareness verification", "showing the real time attack vectors", and "emphasizing the existing security strength of the organization". It helps to improve security policy-procedures [31] and important proactive measures [23] to protect a system. A secured cyber environment ensures not only security but also a sustainable environment. Cyber specialists practice penetration testing to utilize their invested capital, time, and attention to minimize the cost and maximize the throughput by mitigating the risks of the organization. There are a few commonly practiced security frameworks/methodologies that are presented in Section 4.1.

A cybersecurity standard includes a set of practices and technical methods for improving the security of organizations, including physical and cybersecurity [32]. A pen tester can follow any suitable standard that is comparatively more appropriate (details in Section 4.2) to implement in databases, networks, Wi-Fi, applications, etc. Experts always suggest following standardization guidelines that could ensure the best practices [33]. Standardization organizations are continuously improving risk management standards, cybersecurity standards, and penetration frameworks that update guidelines and security baselines. This review article selects frameworks, standards, tools, and vulnerability scoring systems because these are distinguished from the required domains for formal penetration testing (Table 1). An organization should develop a penetration process with an optimal combination of standards, frameworks, tools, techniques, analyses, and reporting systems. Previous studies (Table 1) concentrated on an individual element and focused on a better approach of each element without considering other factors, but this work is aimed at establishing complete penetration guidelines. Further research is required because the studies (Table 1) have not been clarified, reported, or elucidated regarding all penetration requirements. Further study is demanded because of the new tools and techniques that are introduced frequently to face the latest vulnerabilities [34] which are invented every week. There is no comprehensive study that relates all penetration requirements (standards, frameworks, tools, and techniques) thoroughly, though an optimum penetration execution depends on the effective implementation of all requirements. Quality

control and sustainability practices not only ensure the quality of a product but also the best practice and culture for process management [35,36]. An organization improves quality of services, effective process management, and sustainability by executing regular penetration testing that is poorly understood by existing studies. The paper is organized as follows: the research methodology is explained in Section 2, which is adopted in this study. The fundamental concept of penetration testing, its lifecycle, and importance are described in Section 3. Section 4 consists of the penetration taxonomy that shows the mapping between the penetration area and the CIA security tried domains. Moreover, it also explains the common vulnerabilities and respective security measures that should be considered in the penetration process. Section 5, Section 6, and Section 7 describe penetration frameworks, standards, and scoring methods, respectively. Current practices, trends, observations, and the future research scope are mentioned in Section 8, with concluding remarks.

Table 1. Review domains (Source: Article authors).

Domain	Subdomain	Reference	Specification
Methodology/framework for pen test	Open Source Security Testing Methodology (OSSTMM)	[37]	This is basically an audit methodology that is easily adaptable in cyberspace for penetration purposes.
	Open Web Application Security Project (OWASP)	[38–40]	A testing guide concentrated on security for firmware, web applications, and mobile applications.
	National Institute of Security and Testing (NIST)	[41]	A flexible cyber security framework concentrated on risk assessment and mitigation plans that can adapt easily.
	Penetration Testing Execution Standard (PTES)	[42–44]	Security experts developed this to specify tools and techniques based on the penetration domain.
	Information System Security Assessment Framework (ISSAF)	[45]	A framework for developing one's own penetration methodology that can establish a relationship between tasks and tools.
Pen testing standards	Commonly used ISO 27000 family	[46–51]	Concentrate on security in Information Systems, security risk management, and improvement security practices.
	Industry-Related Standard Family	[48,52–55]	Industry standards: ETSI EN 303 645, ISO/SAE 21434, FIPS 140-2, and IEC 62443; concentrate on security in the cyber world and IoT devices.
	BIS standard	[52,56,57]	Developed by the German government, focusing on the security product; three distinguished wings: BIS 100-1, 2, and 3.
Penetration tools	Network scanning	[58–60]	KaliLinux, WireShark, nmap, Metasploit
	Web application scanning	[58,59,61]	Invicti/Netsparker, BeEF, Zed Attack Proxy, Brup Suit, Nikto, W3AF,
	Malware scanning	[58,61]	Nessues, KaliLinux, Acunetix,
	General vulnerability check	[58,61,62]	KaliLinux, Intruder, Metasploit, SQLmap, Acunetix
	Traffic scanning	[58,59,63]	WireShark, Astra, Brup Suit
Penetration scoring methods	Risk Scoring System (RSS)	[64]	Numerical scoring system, poor performance in complex to complex systems.
	Threat, Exposure, Mission, Safety, and Loss (TEMSL)	[65]	Vulnerability remarks: none, some, significant, and it is still in progress.
	Industrial Vulnerability Scoring System	[65,66]	Still in progress, and focusing on industry management.
	Common Vulnerability Scoring System (CVSS)	[67–69]	Numerical scoring, industry standards for IT.

2. Methodology

This systematic literature review is accompanied by the penetration domains of frameworks, standards, tools, and scoring systems by investigating published scholarly articles between 2017 and 2022, besides standardization documents and web articles. This study systematically identified, verified, scrutinized, and extracted the required information for each domain. A cyber penetration process is a complex activity with standards, frameworks, tools, and techniques that varies from enterprise to enterprise. The objective of this study is to analyze existing practices and requirements for executing a penetration test.

Figure 1 illustrates the information selection procedure for each domain that is repeated multiple times until we obtain sufficient research articles from Google Scholar, documents of the standardization organizations, and web portals. Standards and frameworks are explained in the documents of the respective organization and the critical analysis available at the expert's website. This review work is aimed to guide a researcher and security professional for framework, standard, tool, and scoring method selection based on the objectives of a penetration testing area such as networks and infrastructure, web apps and databases, user management, etc. It is going to perform a comparison study among the currents using tools, frameworks, standards, and scoring methods to show the future research and development scope in this realm.

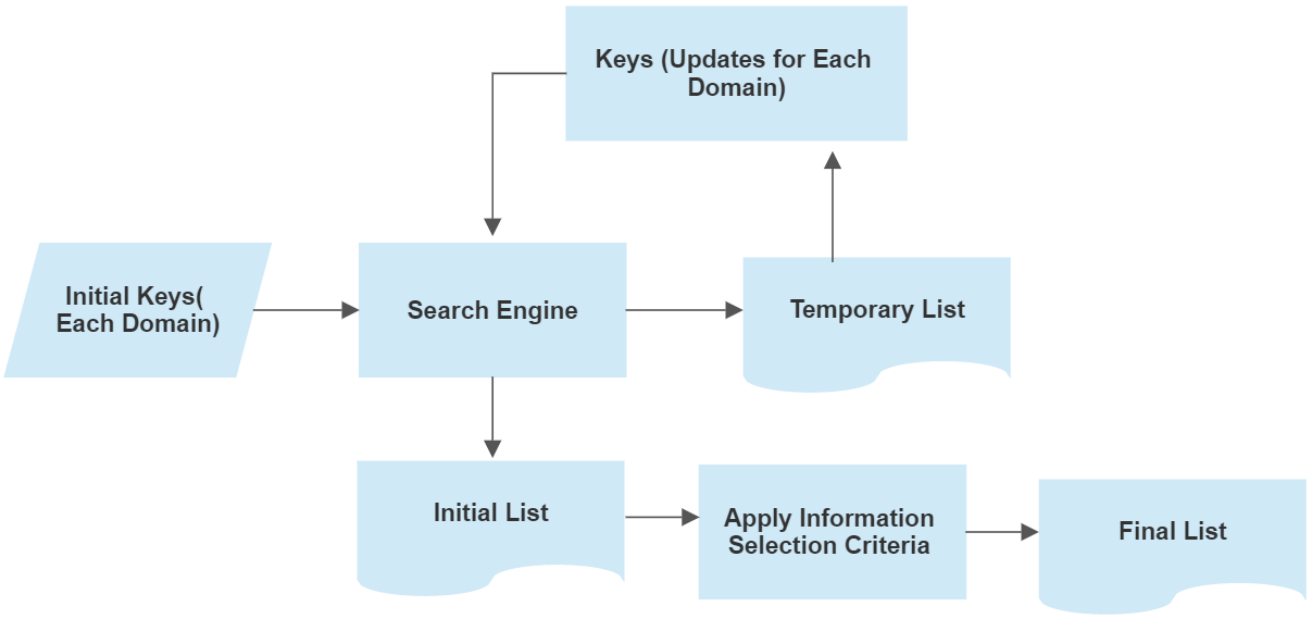

Figure 1. Research Paper Selection Methodology (Source: Article authors).

A popular and potential search engine is selected, which has the ability to search almost all online databases and execute efficient queries. "Penetration Testing Frameworks", "Penetration Testing Standards", "Penetration Testing Tools", and "Penetration Testing Scoring Systems" are the fundamental strings for the search engine query. The top-ranking links for initial queries are mostly websites that consist of standardizing organizations, technical bodies for certifications, promotional companies, and blogs. The modified queries run in the Google Scholar search domain and retrieved from most research articles and initial lists are developed with selected documents. Each article and web document is analyzed and only accepted when it is aligned with any domain of the selective area and consists of relevant updated information.

This paper performs a comprehensive literature review of widely used penetration frameworks, standards, tools, and vulnerability scoring systems. The future research scope is mentioned in the recent trend and observation study in the conclusion section.

3. Penetration

Penetration identifies vulnerabilities of the cyber system so that the organization can implement appropriate protection before any cyberattack. It is an authorized simulated attack [70] against the computer system to check the security posture. It is a special, ethical form of hacking that is becoming a regular practice in the cyber world. A pen tester customizes the guidelines of a standardization document and execution methods from the selected framework to execute penetration activities according to the demand of the organization. The penetration process has a finite set of activities, which is illustrated in Figure 2. Organizations' requirements vary based on business demands and the nature of jobs. An enterprise may want to check only the network vulnerability rather than web applications or databases, and the pen tester should execute the required task based on the guidelines and standards of the network infrastructure and devices, without considering other risks or threats.

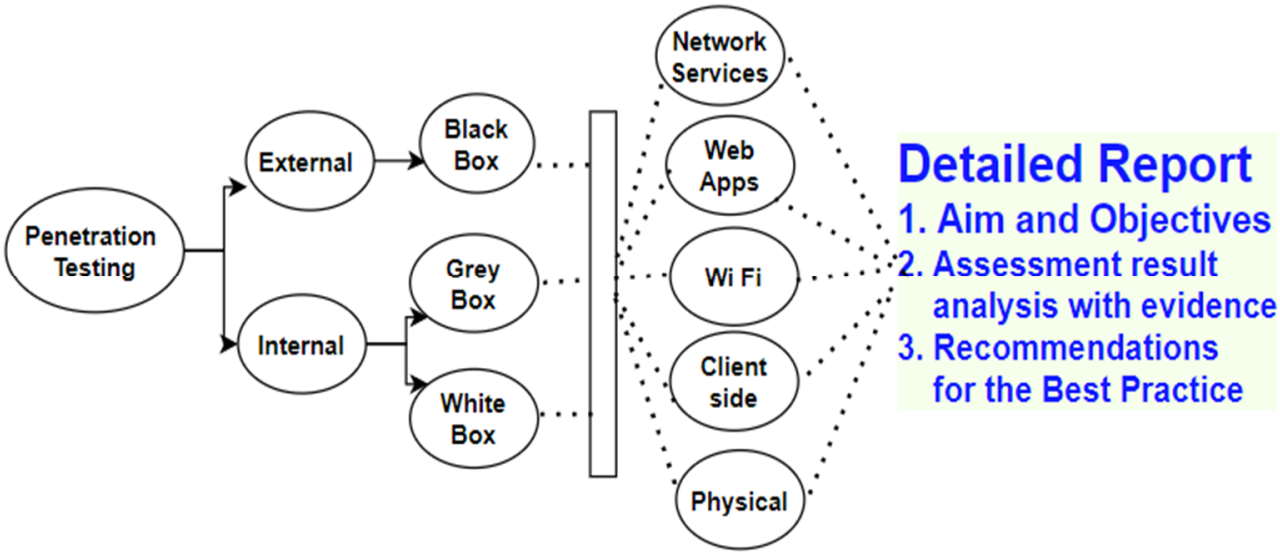

Figure 2. Penetration Overview (Source: Article authors).

3.1. Penetration Overview

Penetration is an official, formal, and ethical practice and deals with sensitive actions that recommend a set of standardization guidelines (Section 4.2) and frameworks (Section 4.1). It could be executed by internal experts or external experts with three distinguished levels of knowledge called black box testing, grey box testing, and white box testing.

A black box testing approach executes penetration with cyber experts who act as real hackers (black hat) and start the attempt without prior knowledge of the information system. The white hat has primary information about the infrastructure and services, while the grey hat has very limited information (publicly published) about the organization. A pen tester collects information by tricking employees, stakeholders, customers, or suppliers, without utilizing published documents or online tools. He attempts multiple attacks on a particular domain and keeps the evidence to generate reports. Similarly, an employee can perform attacks to review the security of a system with full knowledge (white box) or partial knowledge (grey box). It is known as an internal penetration test. During the penetration process, internal employees may be blind or aware of the audit according to the policy of the organization. Penetration includes different tools and techniques for examining the vulnerabilities of the physical environment, client-side machines, WiFi architecture, devices, web applications, and network services, as well as peripheral devices and media. Finally, a penetration report is developed by a pen tester team, including evidence of vulnerabilities, vulnerability scores, and recommendations. The recommendation should show the way of

fixing or minimizing threats. They must fix the system such that the system is like it was prior to the implementation of the penetration process.

3.2. Penetration Phases

Penetration testing considers all possible parts of the information system, but it could be implemented partially too. A penetration tester applies multiple methods of attacks with multiple tools and techniques. A penetration process is structured based on the area of coverage or the depth of testing. There are five major phases (Figure 3) of penetration testing [71] that should be executed sequentially to complete a cycle. It is a regular process, like an audit, that should be implemented regularly (e.g., once yearly), after implementing new infrastructure or even upgrading a system.

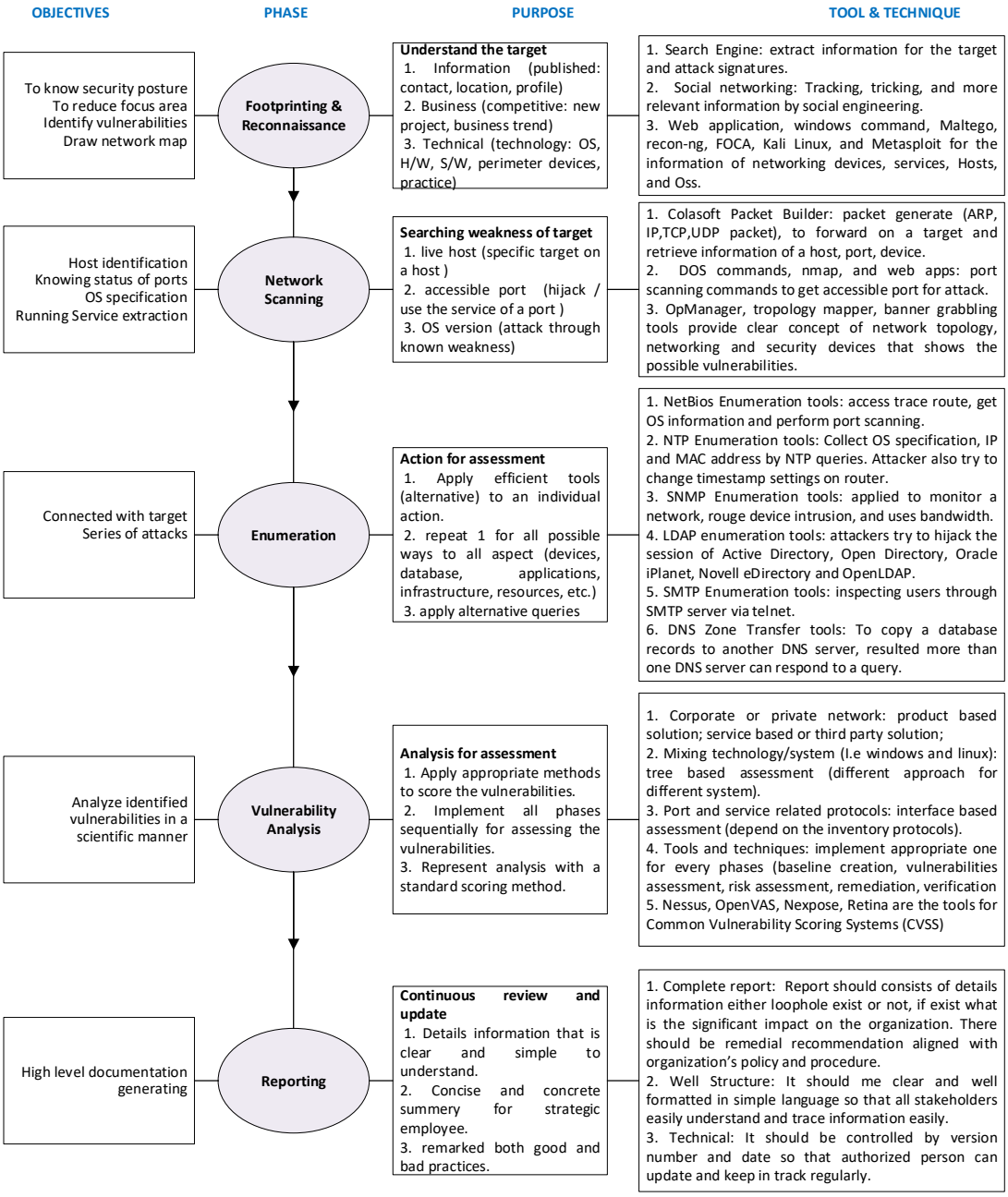

Figure 3. A single iteration of the penetration life cycle (Source: Article authors).

- Footprinting and reconnaissance: This is the first phase of the penetration process, which collects information about the target organization, its technical and physical infrastructure, and users' contacts. Information is collected from users (maybe by tricking too), published documents, online scanning tools, third parties, stakeholders, etc. Attackers want to know as much as possible about the IT infrastructure and services to explore the attacking scope, methodology, and tools. Collected information also supports making an effective attacking strategy and plan. The main aim of this phase is to define the goal and scope of the test and collect relevant information for making an attacking strategy.
- Scanning: In this phase, the attacker will interact with the target to identify prospective vulnerabilities. Attackers make different attempts to scan the information, and their responses are recorded for further analysis. The existing exploitation strategy will be updated according to the results of the analysis. Different scanning applications, tools, and techniques are applied in this phase to scan networks, devices, and services. It identifies an open shared drive, open FTP ports, services that are running, etc. Scanning methods are divided into static scanning and dynamic scanning. Static scanning is aimed at identifying the vulnerable functions, libraries, and logic. On the other hand, in the case of dynamic scanning, a tester passes various inputs to the application and records their responses. Dynamic scanning is more practical and faster than static scanning.
- Enumeration: Attacks are performed in this phase based on the strategy and plan that was developed in the first phase, as well as scanning information from the previous phase. Special knowledge, skills, and experience are required for accessing loopholes to obtain access control. Skills and patience are important for applying a series of attempts to achieve an attacking target by using multiple tools and techniques. An attacker tries his best actions in this phase to extract targeted data, compromise the network's security, and disturb services. The pen tester executes all possible attacks on the system and records all bugs in the applications, networks, memory, social engineering practices, user practices, physical security posture, Wi-Fi, zero-day-attacks, etc. [72].
- Analysis: Risk analysis is performed according to the exploitation evidence of the vulnerabilities in this phase. A tester should follow standard methods for risk measurement and impact mapping [73], with categories such as critical, high, medium, and low, which provide a priority for initiating the fixing of the required vulnerabilities [74]. The analysis report is comparatively short and simple, but it is easy for management to know the system's weaknesses [75]. It also includes clean-up activities such as removing executable scripts and temporary files, reconfiguring the original setting that was used before exploitation, eliminating all installed rootkits, and removing the user accounts that are created by testers.
- Reporting: Usually, it is a formal document of the summary of the entire penetration testing that is submitted by the pen tester team to the organization with a recommendation guideline [74] to enhance the security of the organization. The report should consist of high-level documentation and be easy to understand, supporting further review. The findings (good or bad practices, strengths and weaknesses, etc.) [75] are explained properly so that internal security teams improve the significant security posture. Reporting is an art that reflects the activities, and a good report adds value to the work.

3.3. Importance of Penetration Testing

There is no dedicated communication channel in the internet world that can protect the vulnerabilities of the shared channel. There is no guarantee that the OSs or applications have no loopholes that are deployed in the information system. Human error is not possible to minimize to a level of zero, and we cannot rely on humans, hardware, software, or communication media. We cannot ignore obsolete systems' limitations in terms of security,

sustainability, and performance. Moreover, hackers are introducing new tools or techniques for identifying new weaknesses and exploiting zero-day attacks. An organization attempts to review their systems, identify the flaws, and fix the vulnerabilities prior to the cyberattack, which is wiser than recovering a system after being affected. A pen testing or penetration test is the process for analyzing the physical and logical security system. It identifies vulnerabilities, exploits the system, and recommends the best practices for improving security and sustainability. It provides a scientific report so that an organization can act prior to a cyberattack based on the proposed remediation. Nowadays, an enterprise can conduct a pen test for one or more of the items, such as: security compliance, measuring security posture, and flaws assessments [76]. The penetration test is mandated to comply with the Payment Card Industry Data Security Standard (PCIDSS) [76], Health Insurance Portability and Accountability Act (HIPAA), and General Data Protection Regulation (GDPR). These are the typical standings for protecting data and guidelines for the regular penetration testing practice [76].

Moreover, a secured ICT infrastructure enjoys the benefits of a sustainable environment by reducing unexpected costs of service disruption or disaster recovery. Penetration practices confirm regular monitoring, analyzing, and preventing the system from cyber threats to meet the business goals of the enterprises [77–79]. It supports reducing internal threats [78], improves the awareness of employees regarding cyberattacks and consequences [79], strives to provide secure services [77–79], and protects resources from attackers or malware [79]. The aims of the penetration process are: (i) to confirm resource availability when required, (ii) to ensure that data are safe when processed, stored, and transmitted, and (iii) to protect information from unauthorized disclosures.

Penetration practice is an iterative process that should be executed regularly or based on demand (after deploying a new or upgraded system) to explore new weaknesses and implement effective security patches. Nowadays, penetration is an integral part of the organization that varies from organization to organization according to the complexity, size, and importance of the services. It suggests a stakeholders' awareness program that can protect us from phishing and malware attacks. It should be embedded into the organizations' strategy to ensure best practice auditing and quality control. Penetration practice ensures the quality of service and sustainability by protecting the environment from physical or logical attacks.

4. Penetration Taxonomy

This section consists of a comprehensive study on the penetration domains with the respective threats and possible protection techniques of each domain. It also relates CIA triad areas with respective penetration domains (Figure 4) that support understanding security measures for each penetration domain. The penetration package is decomposed with 12 distinguished domains, which are the major concerns of an organization in protecting the system from internal and external threats.

4.1. Penetration Domains

Review and update security policy: Today, we live in a hyper-connected world that generates several quintillion bytes every day. Data are used in decision-making applications that accelerate services. Hackers not only steal data from the victim for financial gain but can obtain advantages from third parties or nefarious actions. Enterprise security policy and procedure should be framed with a coherent vision and a dynamic set of stratagems. It must include the most likely security threats to a network and the best minimizing practices. A standard organization should utilize a risk assessment matrix, which is an analytical tool that precisely qualifies the safety measure of an industry. The testing system is guided by the laws and regulations that are visible in industries. A good policy procedure must be well-structured documentation that consists of complete and clearly defined rules and responsibilities. In this digital era, there is no industry without digital security policy

procedures that are imposed by the top management for better governance. Security policy must be updated according to the latest national and international digital acts.

Figure 4. Penetration Taxonomy (Source: Article authors).

Educate end users and IT staff and verify their practice: Security breaches come from the technical or physical environment, and there are no specific types of employees beyond the target of attack. However, typical users mostly focus on their job responsibilities without giving priority to the security measures, though they do not like any downtime on the system or any interruption in their service. All users need to be aware of the importance of cyber security, the cyber policy of the organization, and safe conduct. IT policy procedure and cybersecurity education is required for new staff before accessing enterprise resources [25]. Moreover, security policies should be readily available all the time for all employees so that they can avoid doubtful actions and minimize risk.

Review physical security: The human is considered as a critical linchpin in the cyberattack chain [80], and physical security is the primary stage of protection. A strong

physical security system enhances cybersecurity, such as a datacenter being deployed in a restricted area. Physical security aims at protecting assets, people, and property from physical actions or events such as disasters, theft, burglary, vandalism, and terrorism. Losing portable devices with information to a competitor can occur due to the lack of physical security. Physical security should be a part of the complete information security framework. It commences with the identification of restricted areas in the enterprise and is followed by taking appropriate measures. A clear definition and specification for accessing restricted areas reduce the risk of unauthorized access. Visitors should be supervised even in non-restricted areas. A security officer should give special attention to rogue wireless access points, the workstation configuration with logout times, consider locking down end users' workstations, and disable open Ethernet jacks, because these are common and important security issues in a physical infrastructure.

Understand perimeter security: Perimeter security refers to the method of protecting an organization's network frontiers from unwelcomed individuals such as hackers and intruders. Each network should be surrounded by a perimeter that entails threat recognition, pattern analysis, and surveillance detection to ensure effective responses. It suggests taking individual actions based on the trusted zone, untrusted zone, and DMZ zone. Firewall configuration review is one of the most important activities in the penetration test, which includes: traceroutes, access control, port scanning, and architecture [75]. The demarcation point must be a clearly defined aspect of security and responsibility. For example, the security of ISP connections is maintained by the service provider company, vendors should incorporate new images of malware for IDS and IPS, and an organization should manage the internal security posture. Internal security officers confirm the security settings of the network devices (routers and firewalls) with strong passwords, unnecessary ports are disabled, cisco one-step lockdown features are added, security audit features are included, filtering passwords are configured at the level of the OSI reference model, a traffic control mechanism is integrated, etc.

Review password management practices: Users' password practices should be standardized with a set of password management principles. Password storing, managing, and updating are regular practices in an enterprise based on the password management policy. A strong password is difficult to compromise by a brute force attack, and password management policies ensure this for a company. A good password management system defines the minimum length of the password, the combination of case-sensitive characters, digits, and special characters, the regular updating, stopping, and reusing policy, the policy for preventing password sharing, the minimum time for the default password, the login failure policy, and the policy for removing immediately when an employee leaves.

Identification of unnecessary services and ports: Hackers obtain additional attack surfaces on open applications or ports that are in the listening mode, and a black hat can exploit a network to breach security. The existing flows of network services support utilizing "service libraries" to compromise the security perimeter. Improper access control configuration, default configuration, or a weak encryption system may cause a Denial of Service (DoS) attack to render a device or block a service. A security employee must ensure a service only when it is necessary for a particular type of user. When black hats attempt to compromise a host, they often look for a known vulnerability of that host, and it may be an open port or service. End users should be restricted to downloading and installing applications as they like. Network firewall and end user firewall implementation can reduce cyber threats. Regular system scanning and disabling unnecessary services and/or ports improve the security posture, quality of service, and sustainability of a system.

Recheck patch management practice: Technology is upgrading and changing rapidly, and applications are also improving their security capabilities with respect to the latest technology. So, keeping the system up to date is a regular activity of an IT team in ensuring better service and security. In addition, new vulnerabilities are introduced daily, and vendors are trying to patch. Black hats also scan the network with known vulnerabilities of existing devices or services. Patch management is a patch installation process (updated

codes) for fixing bugs, improving the service, and reducing security holes. Patch management includes updating a system, testing the system, and maintaining documentation for each patch. As a result, a sustainable cyber environment is ensured by patch management.

Review antivirus measures: Antivirus software is designed and developed to detect and remove viruses from computers. It can also protect malicious attacks such as keyloggers, rootkits, spyware, botnets, adware, Trojan horses, etc. An organization should install antivirus software on workstations, gateways, firewalls, servers, and end user machines. They should use enterprise antivirus management software and be constantly vigilant such that they have the latest antivirus signature. Antivirus management systems should be active to generate alerts.

Effective access control: Access control is an information security process for protecting data and resources from unauthorized access. It is physical or logical. Physical access control is managed by policy procedure and physical security measures for the restricted areas; the logical access control system assigns the users and their rules on the network. Logical access control includes an authentication system for identifying a unique user and an authorization process for assigning privilege of access to the users. The access control system manages users' confidentiality by assigning and updating rules and privileges. It also performs regular audits and user data analysis to search for abnormalities. The administration can assign group user rights rather than individuals that need their job on selected files, directories, and devices. Security teams need extra care to give remote access. Site-to-site and client-based VPNs can ensure secure access through insecure communication channels.

Secured data transit: Cyber security achieves the confidentiality, integrity, authentication, and non-repudiation of digital data communication with cryptographic and hash algorithms. This ensures data availability to the right person without any modifications. A secure data transaction system maintains users' privacy, and there is no scope to deny any action that is already taken by a user. A client-based VPN allows you to create a secure network between users and a remote network, and a site-to-site VPN allows for a secure connection between two different physical networks. For wireless communication, administrators can implement WAP2 secure protocols to end user devices and enterprise networks. Secure web transaction services can protect the communication of an untrusted zone.

Review IDS and IPS implementation: The IDS monitors the network traffic and provides alerts about a potential security incident, and the IPS prevents malicious actions in a network. The Security Operation Center (SOC) analyzes the alerts that are received from IDS to know the tendency of unexpected packets so that they can take the required actions. An administrator can install a host-based IPS in the host machine to protect users' information and a network-based IPS to the firewall to protect the network. A security employee can implement a signature-based approach in the IDS and IPS by using predefined signatures of well-known network threats to protect themselves from known threats. When an attacker initiates a threat to the network, the IDS/IPS will detect that it is identical with predefined signatures, and the IDS/IPS will take necessary action. In the anomaly approach, there is no predefined signature to match with incoming packets, but the IPS/IDS uses intelligent analytics to detect reasons for abnormal network traffic.

Review data backup systems: The preparation for backup implementation is not an overwhelming task or not willing to accept a disaster; it is a precautionary measure. Data backup is a reliable and sustainable service for delivering data when they are needed. Backup data support the organization after any incident of physical or logical damage. Cyber security strategy and policy include backup and recovery technologies, principles, rules, regulations, and responsibilities. Security experts always choose an automatic data backup solution. According to their data policy and the importance of the data, a company can implement one or more well-known data strategies: "enterprise solution", "imaging solution", and "SOHO solution".

4.2. Penetration for Common Vulnerabilities

Cybersecurity attacks are serious threats to the bottom line and public reputation of a business. A penetration process should focus on common and recent attacks so that the organization can minimize the risk from the recommendation of the test. This section consists of some common vulnerabilities, their impacts, and remediation.

Password attack is a common form of a cyber-attack that could act as a brute force attack, dictionary attack, rainbow attack, password spraying attack, credential stuffing attack, and attack with a keylogger [25] to extract a victim's password. A keylogger is a malware application that records all information related to stroke keys, visited websites, and accessed applications; this recorded information is accessed by hackers who can use the credential information to use it against the victim. It leaks credential information such as the ID, password, pin, and credit card information that could be used by hackers [81]. Cryptanalysis is the process used to decrypt a message without knowing a secret key. It is also used to generate passwords for dictionary attacks, brute force attacks, and rainbow attacks [82]. A dictionary attack attempts to obtain a password by trailing guessable passwords of a password dictionary, but it fails when the password is strong, with characters, digits, and symbols [82]. A brute attack tries to retrieve a password with possible numbers of permutation and a combination of elements (length, digit, character, special character) based on the policy of an enterprise. It is very difficult (higher time complexity) to extract a password, and it may take more time than the session time of client–server communication. Shoulder surfing is a physical attack for obtaining a password by observing a user's login action [83]. Attackers try to obtain the hash value of a password from the database, which is called a rainbow table attack.

Malware is a malicious computer program that disrupts or damages the system with a variety of working principles [24]. Viruses are the malware applications (Table 2) that can destroy data, hard disk partitions, or the functionalities of the peripherals when they are executed by a host [84]. Worms replicate the files of a computer system to consume resources so that the system will crash or become inactive. The trojan horse is a special kind of software that allows for backdoor entry through a covert channel [84] so that a hacker can exploit the systems. Hackers can install malware with spear phishing techniques to create backdoors for the exploitation of the system [25] and can lock a system with malware to obtain ransom [24].

Table 2. Common viruses and their protection measures (Source: Article authors).

Virus	Way of Affecting	Way of Spreading	Way of Protection
Boot sector virus	Overwrites/installs code with the boot file.	Through physical media, mostly.	Stop the initial payload from installing and use a good anti-virus.
Parasitic virus	Attaches itself to the exe. file and delivers a payload when the program is executing.	Mostly online links and documents.	Avoid unsecure Wi-Fi and clicking links without being sure; use anti-virus.
Stealth virus	It averts anti-virus scanning and hides itself. It attacks the OS processes.	Downloaded through email attachments or unverified software.	Use up-to-date strong anti-virus signatures.
Polymorphic virus	Makes a copy of itself when coming in touch and updates the copies.	Creates and modifes its version as well as encrypts their codes that are different from each other.	Preferable cloud native environment; use up-to-date next-generation anti-virus software as well as pop-up blockers.
Marco virus	Infects Microsoft Office files and OS that can transport between different OSs.	When an infected document is shared and forwarded.	Strong anti-virus software and awareness about email phishing are preferable.
Multipartite virus	It can infect more than one way, both programs and boot sectors.	Typically spread by attaching it to a self-executable file.	Avoiding clicking on suspicious links, use reliable anti-virus software, and keep a backup.
Spawn/companion virus	It does not physically touch the files.	Self-copy is saved by the name of another file with a different extension.	Prevention measures of the virus.
Web scripting virus	Stand-alone file that could be executed by the interpreter.	Spread through infected websites and steals data or damages file.	Secure web browser, antivirus software, and cyber security measures.

Social engineering is the art of manipulation, motivation, and convincing tricks that are applied to the users, and they share their confidential information with the attacker. The attacker generally sends bait in the form of an email message, and the victim accepts it as authentic information and takes necessary actions based on the guidelines of the email or message. As a result, a hacker obtains the required information for hacking, which is called a phishing attack [24]. Organizations have a standard password policy, and they have trained employees. However, social media platforms do not apply strong password policies to keep things simple and achieve business goals. A hacker can obtain the password of a social media account of a target easily [25].

An eavesdropping attack or man-in-the-middle attack attempts to hijack a session between client and server communication. This is known as "sniffing" and "snooping", when an attacker searches for the weakness of the system for backdoor entrance [83,85]. A hacker is a person who intends to extract victims' information by intercepting the communication channels of two persons [25]. An attacker stores the information that he can obtain from communication devices that may be confidential to a user, and the attacker can use it for further malicious actions [81]. A hacker uses a client's IP to communicate with the server, and the server usually responds. Currently, encryption technology is applied in emails or instant message passing applications [86] to protect data in transmission so that the data cannot be used for malicious actions.

Denial of Service (DoS) attack is an intention to intrude on the networking services of an organization. It attempts to flood the network traffic by forwarding unnecessary data packets to the target network. As a result, desired bandwidth is consumed and exhausts resources, but it is unable to stop the services. A distributed denial of service (DDoS) attack is performed by a group of malicious machines (Botnet) [24] together regarding a victim, which creates several times more traffic than a DoS attack on a network [82,84]. It is used to attack an enterprise that has a cluster of servers, and one machine is not sufficient to attack. The Botnet method is applied to increase the number of attacking machines in DDoS attacks to increase the victim's suffering, and a hacker becomes happy if he can stop the original requests of the targets [86].

Code injection is a form of cyberattack that manipulates standard SQL queries for database-driven web applications to compromise the security of those applications [81]. Attackers want to insert malicious code into the SQL servers to retrieve information. Cross Site Scripting (XSS) is an attacking technique of website hacking involving injecting malicious code that has different approaches: reflected XSS executes the malicious script on clients' machine, and the server does not store it; the stored XSS approach stores and executes the malicious script on the server that is executed by multiple users [25,31]. Document Object Model (DOM) XSS is a client-side attack that executes malicious code after the execution of a legitimate server script. An attacker identifies the appropriate method of SQL injection; for example, the appropriate webpage-code-injection method is applied by analyzing the design of the targeted webpage [82].

5. Penetration Frameworks

Penetration frameworks suggest applying a systematic penetration process to find out the weaknesses and loopholes of a network of the enterprise prior to a cyberattack. This activity is accomplished through an iterative process known as penetration testing or, simply, a pen test. Simply, it is the art of achieving vulnerability identification as much as possible by entrancing into the inner system to reach the target. A hacker always tries to compromise barriers so that he can act as a legitimate user. The pen testing framework includes security compliance verification and staff awareness confirmation. A penetration test explores the vulnerabilities and shows the real-time attack vectors, which show the existing security strength of the organization. It discusses scanning for major vulnerabilities and suggests improving security measures. So, a standard organization practices pen testing regularly (i.e., yearly) or when any change (e.g., any newly installed system or any device is updated) is incorporated in any device in the system. A framework recommends

following guidelines to execute a penetration test, to develop a list of vulnerabilities according to the priority, and to fix them based on the priority. A pen tester can help to improve security policy and strategy with respect to the prioritized vulnerability list, the tools that were used in the test, and the proposed remediation [31]. Penetration minimizes the security issues of an organization by accepting proactive security measures, improving security and sustained services [23]. Table 3 represents five commonly used penetration testing methodologies [87].

Table 3. Penetration Frameworks (Source: Article authors).

Penetration Methodology	Description
Open-Source Security Testing Methodology Manual (OSSTMM) [37]	Features: IOSSTMM is an audit methodology for security testing that is adaptable to vulnerability assessment, penetration testing, or ethical hacking. Version 3 (the latest one) of OSSTMM is developed to execute penetration testing for physical and virtual infrastructure, middleware, clouds, networks (mobile, telecommunication, wireless), humans, and data handling issues. It performs security tests at the operation level and does not concentrate on anecdotal evidence or assumptions. There is a set of attack surface and visualization tools for comparative analysis. It also includes a quantitative risk assessment facility. Advantages: It welcomes anyone to an open-source system testing process that shows repetitive and consistent results. It could be integrated with existing laws, policies, and industry regulations. There is guidance to protect the intellectual property of the organization. Disadvantages: The repetitive work increases the complexity, time, and cost as well as the additional effort required to adopt the methodology in the penetration process. Before starting the penetration test, a tester needs to read and understand all processes clearly for adaptation to the system. It focuses on the certification of a security tester and organization.
Open Web Application Security Project (OWASP) [38–40]	Features: It has three different testing guides based on the type of application, and these are: OWASP Web Security Testing Guide [38]: It concentrates on the software development process and on reducing bugs in the applications. A developer can utilize this to produce secure code and for quality assurance. A software tester can check the software before the release, a project manager can incorporate it to maintain the overall security of the enterprise, and a security expert can verify the security holes. OWASP Mobile Application Security [39]: It provides a service for testing, checklists, test cases, and reverse engineering to review a system, and its working principles are updated regularly. It is guided by a Mobile Application Security Verification Standard (MASVS) that could be used by a mobile app developer, tester, architecture designer, and mobile security professional. It suggests adding test cases for all requirements and tracking compliance for practical assessment. This guide consists of specific guidelines for the Android platform and the iOS platform besides the general guidelines for the vulnerability testing. Reverse engineering, tempering techniques, and prevention methods are incorporated in every case. OWASP Firmware Security Testing Methodology [40]: It is constructed to explore victims' firmware and examine the features of that firmware. It extracts the characteristics, carves, emulates, and analyzes the content of the file system of a targeted firmware. It is used to execute dynamic security tests of firmware from the interface and analyze runtime binaries or binary exploitation to attain at the root. Moreover, it is now extended to mobile apps that deal with Internet of Things (IoT) and cloud-based information. Advantages: It is highly application-oriented, and it concentrates on the development process, coding, and testing of web-based software, mobile applications, and embedded systems. Integrating security features into a product is the main purpose of this framework. It is also commonly used as a penetration testing framework. Disadvantages: It is mostly concentrated on applications' security rather than organizations' security.
National Institute of Security and Testing (NIST) [41]	Features: The NIST cyber security framework consists of three main components: the framework core, framework implementation tiers, and framework profile for risk management. Identification, protection, detection, responding, and recovery are the five continuous functions of the core of the framework. It remarks discrete outcomes of subcategories for each function and attempts to match with existing industry standards, practice, and guidelines. It tries to communicate from the strategic level to the operation level on account of the security purposes of the organization. Framework implementation tiers describe the degree of an organization's cybersecurity practices (i.e., risk management and threat awareness practices, repeatable and adaptive processes). An organization is categorized from tier one to tier four based on the current security practice, threat management, legal and/or regulatory limitations, the business objective, and the constraints of the organization. These outcomes guide a team in developing recommendations for further improvement. An organization can select categories and subcategories from the framework, where a framework profile shows the assumed outcome according to selected categories and subcategories. The profile is aligned with standard guidelines and practices that help to improve the security posture of the current system. A current profile could be used to prioritize and measure the progress towards the target profile. Advantages: This is concentrated on the risk assessments and could be adapted to any organization by selecting categories and subcategories from the framework. Business missions are reinforced in each component of the framework that supports enhancing business security and achieving business goals. Disadvantages: A pen tester needs a very good idea of the framework and the security requirements of the organization before adapting the framework.
Penetration Testing Execution Standard (PTES) [42]	Features: It is developed by security experts for seven consecutive steps: pre-engagement interactions or initial communication to know the reasons for pen testing; the intelligence gathering phase collects information of the system; the threats modeling step identifies the existing threats; vulnerability analysis is performed to select the required tools and techniques of exploitation; evidence exploitation and keeping the evidence; analysis of the impact of exploitation on the organization; and developing a detailed report with recommendations. Advantages: It supports a technical guide [43] that specifies tools, domains, and techniques for the penetration test. It tries to develop a minimum baseline for the pen test that cannot cover all scenarios [44]. It generates executive and technical reports for the enterprise [44]. Disadvantages: This is comparatively new, and, until now it has been in the improvement stage. It can be implemented by businesses and security service providers [42].
Information System Security Assessment Framework (ISSAF) [45]	Features: ISSAF is aimed at delivering a comprehensive guide to developing our own pen test methodology that links each step of the penetration test with a specific tool [45]. There are three steps in ISSAF: Step 1 performs the identification of a communication channel between an organization and a pen tester company; it detects the scope, approach, and methodology for execution, and it performs agreement for penetration based on the test case and escalation path. Tools and techniques are explained in Step 2 to specify the targeted area such as the application, database, network, and hosts. It illustrates the detailed scope of the penetration test that is well defined and structured with the process of execution phases. Finally, a complete test is performed in this step. Step 3 is quite brief and focuses on removing the artifacts that are created during the penetration test as well as developing technical and executive reports. Advantages: It establishes relationships between tasks and respective tools. Disadvantages: It is not maintained properly and is a little bit out of date [45].

6. Penetration Standards

Cyber risk is available in all infrastructure but the severity of the risk is not the same [88] and we practice standardization guidelines to minimize existing to manage-

able level [89]. Penetration standards ensure the implementation of a set of practices and technical methods to improve security in networks, storage, internet, hardwires, and software for its users [32]. It is aimed at reducing cyberattacks [90] and improving business goals [32]. Cybersecurity experts recommend integrating security standards so that organizations can ensure the best security measures to minimize cyber risk [33]. A standard specifies processes, procedures, guidelines, and baselines for security control [91]. Cybersecurity standards have been applied to different organizations to perform penetration testing [92,93]. Standards can guide the reviewing process and improve formal practices [56]. Table 4 consists of commonly used cybersecurity standards.

Table 4. Penetration Standards (Source: Article authors).

Standard	Features
Commonly used ISO 27000 family [46]	The International Electro Technical Commission (IEC) and International Organization for Standardization (ISO) published the ISO/IEC 27000 series that concentrates on the security of information systems management (ISM) [47]. 27001:2013 has seven steps (installation, operation, monitoring, controlling, maintenance, review, performance, and improvement) that can lead to improved information security practices in business organizations [56]. It supports managing business information and personal information secretly, which can improve the branding of an enterprise [94]. The organization's assets are securely managed and protected by 27002:2013. Moreover, the personnel, operations, business continuity, compliance, and information of an organization are protected by the guidelines of 27002:2013 [49]. A responsible individual can implement the best practice recommendations of 27002:2013 to improve the security posture of an enterprise [50]. Organizations implement 27005:2018 for cybersecurity risk management with the standard ISO/IEC 27001. ISO/IEC 27005 has employed seven elements in the risk management process [49] that ensure risk mitigation at a satisfactory level, though it depends on the skill, practice, size, sector, and budget of the company [51]. 27006:2015 was initiated for information security certification management by a third party to enhance the trustworthiness of the organization [56]. Information security standards are specified as ISO/IEC 27003:2017 (guidance), ISO/IEC27000:2018 (vocabulary), ISO/IEC 27007:2017 (auditing), ISO/IEC 27004:2016 (monitoring, analysis, evaluation), ISO/IEC 27014:2013 (governance of information security), ISO/IEC 27017:2015 (code of practice) [49], etc.
Industry-Related Standard Family [52]	ETSI EN 303 645, ISO/SAE 21434, FIPS 140-2, and IEC 62443 are commonly used by industry standards for special purposes in industry risk mitigation [52]. ETS EN 303 745 mainly concentrates on the policy procedure development for Internet of Things (IoT) management devices [53]. It includes all stakeholders who are related to IoT-based product manufacturing and application development [53]. The ISO/SAE 21434 standard is applied to manage risk and protect road vehicles from cyberattacks. It is extended to minimize risk in the process of vehicle production, development, and maintenance [54]. FIPS 140-2 defines four security levels known as secure cryptography modules that are accepted by federal agencies of the United States and Canada [48]. IEC 62443 consists of a series of international standards for cybersecurity in industry automation [55]. It has different categories to meet the threat protection in the area of cybersecurity.
BSI Standard [56]	*Bundesamt für Sicherheit in der Informationstechnik* (BSI IT) is developed by a German government agency [52] that is responsible for the security of digital communication and computers. It also focuses on the security products, security labs, and security processes [56]. BSI 100-1 describes a few mandatory requirements that are integrated with ISO 27001 to ensure the security of IT infrastructure [56]. The BSI 100-2 standard concentrates on IT security management, step-by-step task implementation for security, and integrating the best practices, while BSI 100-3 is developed for risk analysis based on *IT-Grundschutz* principles [57].

The automated penetration test saves time, but it will throw off several false-positives, and a good pen tester performs a manual review too [95]. Sometimes, an environment does not support it due to disruption, a lack of test accounts, and limited resources and scope [95]. However, since a considerable number of standards have been developed to cover different aspects of cybersecurity in various organizations, it may be challenging for business owners to choose the appropriate standard [96]. Frameworks provide guidelines and standards specify the required actions for an individual domain, such as risk, policy,

industry automation, etc. This paper concentrates on the general penetration test so that any organization can adapt as they like.

7. Penetration Tools

Information security is more than just IT protection; it is a part and parcel of business culture in obtaining competitive advantages in this digital economy. It is also not a matter of confirming secured information systems once and enjoying the service for a long period. New vulnerabilities are explored by hackers regarding the existing hardware, OS, medium, or applications, besides inventing new malware. So, a cyber-security team should be up to date with the latest threats' images to protect computing resources. A pen tester needs to utilize appropriate and updated tools to review the vulnerabilities [58]. In this section, we compare commonly used penetration tools.

- KaliLinux 2023.1: In most cases, it is considered as a default penetration. OS [59] is a reliable pen-testing tool on the platforms of desktops, mobile devices, virtual machines, Docker, and Windows or Linux-based subsystems [60]. It supports vulnerability scanning and digital forensics operations and can be used as a sniffing tool for LAN and WAN [61]. In addition, it is used for 16-bit brute force password cracking [61].
- WireShark 4.0.6: It is an open-source application that is used to monitor network traffic [58]. It can capture Ethernet live-data [61] and inspect USB data [58].
- Intruder: It is a common tool used in the banking and government sector to scan vulnerabilities of the system [58]. It performs auto analysis and develops a vulnerability list based on the risk priority [62]. It is supported by ISO 27001/27002 standards and SOC 2 compliance standards [62]. Moreover, it can work with cloud systems: AWS, Google Cloud, and Azure [62].
- Astra 5.3: It is a comprehensive penetration testing tool for manual and automated tests [58,59,61], with more than 3000 tests that can integrate CI/CD with other applications [58]. It is enhanced with an interactive dashboard for the compliance security test [63].
- W3AF1.6: This is a Python-based web penetration tool with a great graphical interface [58] that is a comparatively easy and powerful tool for developers [61].
- NMAP: This is one of the most popular network scanning tools used for port scanning, network mapping, and creating inventory for network services [58]. Network administrators also use this as a regular testing tool for monitoring, inventory management, service management, and upgrading schedules [60]. In addition, legitimate organizations scan the entire IPv4 range and ports regularly for the IP map and ports' status respectively [59].
- Metasploit: This is one of the most-used automation frameworks for penetration testing [61], which consists of 25 platforms with more than 500 payloads and 1677 exploits for vulnerability checking [58]. It also performs real-time analysis and supports decrypting hundreds of protocols [59].
- SQLmap: It is applied in automated penetration to detect SQL injection flaws [58] with Boolean, stack, union, and error injection methods [61]. It supports H2, Informix, MaxDB, SAP, Microsoft SQL Server, MySQL, Oracle, PostgreSQL, Microsoft Access, SQLite, IBM DB2, Firebird, and Sybase for security checking [59].
- Nikto 2.1.6: This is an open-source pluggable web server scanner that consists of 7000 scanning programs [58]. There are plenty of tests for both vulnerability and misconfiguration tests.
- Nessues 10.3.0: It is an ideal tool for malware and missing patches identification [61] that consists of more than 65,000 vulnerability tests. It could be integrated into tenable products and services that are regularly updated [58].
- Brup Suit 2023.4.4: It is an open-source tool that is incredibly effective for web traffic exploration and can fire when required [59]. It consists of a set of tools such as a web crawler, repeater, sequencer, and proxy to perform security tests on web applica-

tions [58]. It is also good for beginners to understand traffic exploitation in a computer network [59].

- Acunetix 15: It is an automatic pen testing tool that is capable of identifying out-of-band vulnerabilities [61] and is applicable for on-premises or cloud platforms [61]. It supports important standards such as PCI DSS, HIPPA, and ISO 27001 and is seamlessly integrated with the platforms: GitHub, Bugzilla, JIRA, Azure DevOps, and Mantis [62].
- Zed Attack Proxy 2.12.0: This is an Open Web Application Security Project (OWASP)-founded pen testing tool for Linux, Mac, and Windows [58] that runs into the entire platform to create a proxy between clients and webpages [61].

Besides these, Aircrack 1.7 is used for packet capturing and data extraction and cracks the flaws of a wireless system [61]. BeEF is used to check the security issues in web browsers [61], and a tester is used as an additional attack vector to know the posture of a target. Ettercap is used to generate a data packet for a man-in-the-middle-attack [61]. Invicti/Netsparker is an automatic web application scanning tool that can scan more than a thousand applications in a day [61]. Moreover, a huge number of web applications and APIs are available for performing scanning or executing exploitation in a sever, network, website, or device.

8. Penetration Scoring

A penetration test is aimed at remediating the vulnerabilities, but it is incredibly difficult to patch every single vulnerability of a system. All vulnerabilities do not have the same effect on the system, and their fixing cost also varies. Even if an organization wants to forgo patches on some vulnerabilities to improve their security, they need to know the priority of the vulnerabilities, relevant cost, complexity, and fixing time. A penetration tester must prioritize the vulnerabilities or remediation with some metric values. The cyber vulnerability scoring system is initiated by the risk scoring system and a compliance scoring system such as "Payment Card Industry Data Security Standards (PCI DSS)". There are dozens of scoring systems, and all of them are unique in their goals and methods. The most common and recent scoring systems are summarized in Table 5.

Table 5. Common Scoring Systems (Source: Article authors).

Method	Scoring System	Application Domain	Limitations
Risk Scoring System (RSS) [64]	Provides a numerical mean score of vulnerabilities	Medical, Commercial Aviation, Weapon System	Fails for complex-to-complex systems
Threat, Exposure, Mission, Safety, and Loss (TEMSL) [65]	Vulnerabilities are ranked with quality terms: none, some, and significant. It uses a decision tree to show the priority.	It is applicable where qualified priority (never, next, now) is suitable.	Not standardization: still in progress [65]
Industrial Vulnerability Scoring System [66]	It calculates the final score based on four different scores.	Focusing on applying it in the industry security scoring management.	Not standardization: still in progress [65]
Common Vulnerability Scoring System (CVSS) [68]	The latest version (CVSSv3.1) calculates scores for three different areas: Base, Temporal, and Environment metrics.	Industry Standard and focuses on IT fields. Could be adjusted in any industry for risk assessment.	Some experts believe that it is difficult to draw the conclusion from temporal and environment scores [68].

The Common Vulnerability Scoring System (CVSS) supports a pen tester in standardizing the vulnerabilities with a scoring methodology, and it is agnostic regarding any platform [67]. It is an open framework exhibiting a characteristic of a system with a score that is developed by the Forum of Incident and Response Teams (FIRST). It is considered an industry standard vulnerability scoring system [67,97] and is commonly used in security companies for vulnerability assessment as well as risk management [97]. A pen tester can utilize CVSS scoring systems to represent vulnerabilities in software, hardware, and firmware with evidence. CVSSv3.1 is the latest version of the CVSS series, which consists of a "base metric group", a "temporal metric group", and an "environmental metric group" [69]. CVSS has been updated (Table 6), and the latest version (CVSSv3.1)

will be released in June 2019 [97]. Table 6 illustrates the improvement of version 3 over version 2 and CVSSv3.1, which does not introduce major changes except for reformulating the equation.

Table 6. Comparison Study of CVSS Versions (Source: Article authors).

CVSSv2	CVSSv3.0	CVSSv3.1
The score reflects the impact of the vulnerabilities on the entire system.	The score reflects the impact of the vulnerabilities on the impacted components of the system.	The score reflects the impact of the vulnerabilities on the impacted components of the system.
This version does not consider environment metrics.	The vulnerabilities that are related to the environment of the application are considered.	The impact of the CVSSv3 environment metrics is modified for subgroups.
There is no indication when a vulnerability affects more than one application in a system.	Scope metrics indicate when a vulnerability impacts other applications in the same system.	The vulnerable and impact components are reformulated and clearly indicated by the scope metrics.
The impact of a vulnerable application is reflected by impact metrics.	Impact metrics are reflected by the impact degree (none, low, high).	The impact metrics score the result of an exploitation.
Authentication metrics may ignore many aspects of vulnerability.	The importance of privileges is reflected by a privilege attack.	A privilege score is generated by an attacker after exploitation and compared with the previous score.
Access complexity includes the user's interaction and configuration of the system.	The complexity of the user interaction and attacks is separated in access complexity.	It demolishes the description ambiguity of the access complexity.
An attack vector can consist of physical hardware and a local access system.	Attack vector metrics separate the local complexity from the hardware complexity of the system.	Attack vector metrics are reformulated for the description values of the local, network, and physical components of the system.

8.1. Base Matrix Taxonomy

The base metric has three major elements: the scope (identify the impact of local system-associated components), impact metric (measure total impact according to the CID triad), and exploitability metric that performs vulnerability actions in the system. Its functionality is illustrated in Figure 5 and Equations (1)–(4).

$$BMc = \{EM, IM, S\} \; where \; EM = \{\}$$

$$ISS = 1 - [(1 - C) \times (1 - I) \times (1 - A)] \quad (1)$$

where BM represents the base matrix, EM represents the Exploitable Matrix, IM represents the impact matrix, S represents the scope, C represents confidentiality, I represents integrity, and A represents availability, and the equations are standardized by different organizations [65,66,69,97]. The Injury Severity Score (ISS) (Equation (1)) is used to calculate the impact of the vulnerability on a system (Equation (2)).

$$impact = \begin{cases} 6.42 \times ISS, \; scope \; is \; unchanged \\ 7.52 \times (ISS - 0.029) - 3.25 \times (\mathrm{ISS} - 0.02)^{15}, \; scope \; is \; changed \end{cases} \quad (2)$$

$$E = 8.22 \times \mathrm{AV} \times \mathrm{AC} \times \mathrm{PR} \times \mathrm{UI} \quad (3)$$

where the Exploitability is (E), the Attack Vector is (AV), the Attack Complexity is (AC), the Privileges Required is (PR), and the User Interaction is (UI).

$$BaseScore = \begin{cases} 0, \; \mathrm{Impact} <= 0 \\ \mathrm{Roundup} \; (\mathrm{Min} \; [(\mathrm{Impact} + \mathrm{E}), \; 10]), \; \mathrm{Scope \; is \; Unchanged} \\ \mathrm{Roundup}(\mathrm{Min} \; [1.08 \times (\mathrm{Impact} + \mathrm{E}), \; 10]), \; \mathrm{Scope \; is \; Changed} \end{cases} \quad (4)$$

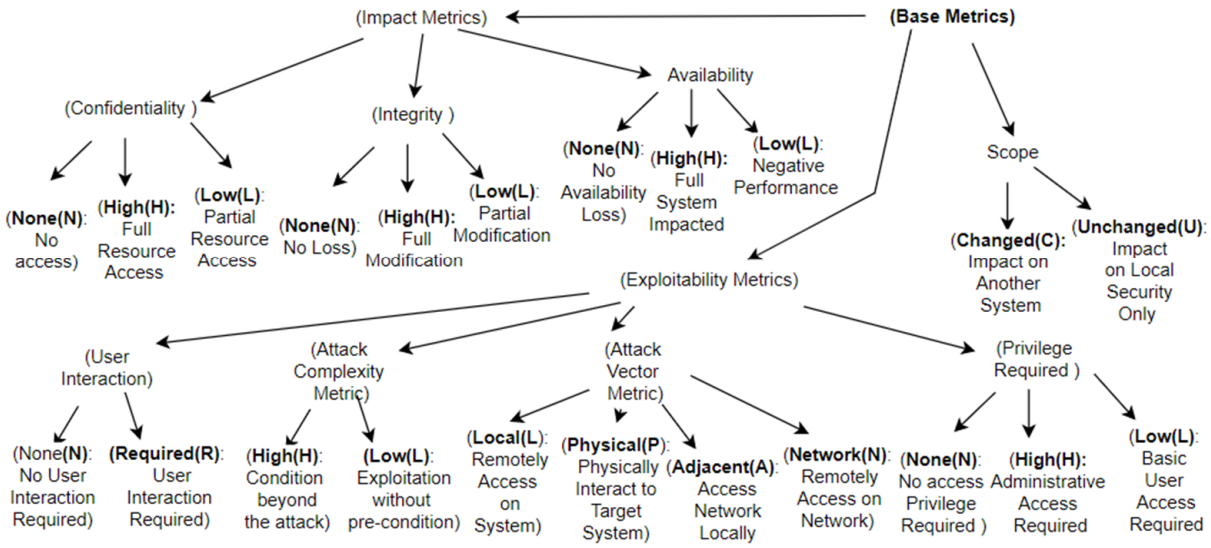

Figure 5. Base metric taxonomy for CVSSv3.1 (Source: Article authors).

8.2. Temporal Matrix Taxonomy

This metric explores the security practice and the level of maturity according to the standards of documentation, the code, and the quality of remediation. Figure 6 and Equation (5) express the elements of the temporal metric. The Temporal Score (TS) is calculated by the Base Score (BS), Exploit Code Maturity (ECM), Remediation Level (RL), and Report Confidence (RC) (Equation (5)).

$$TS = \text{Roundup}(\text{BS} \times \text{ECM} \times \text{RL} \times \text{RC}) \quad (5)$$

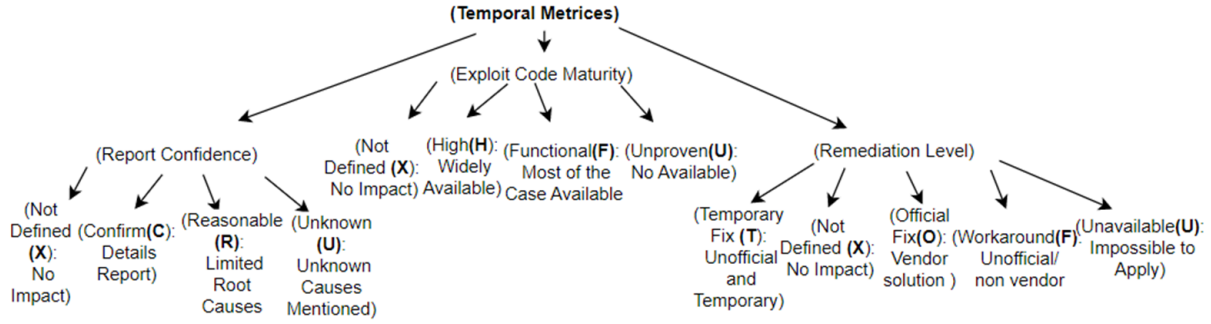

Figure 6. Temporal metric taxonomy (Source: Article authors).

8.3. Environmental Matrix Taxonomy

Figure 7 and Equations (6)–(8) figure out the facts of environmental metrics that have a direct impact on integrated technological elements with a vulnerability. The Modified Injury Severity Score (MISS) is calculated by Equation (6), based on the confidentiality, integrity, and availability. CR stands for the Confidentiality Requirement, IR stands for the Integrity Requirement, and AR stands for Availability Requirements. The Modified Impact (MI) (Equation (7)) is derived from Equation (6), and Equation (8) calculates the Modified Exploitability (ME), which only depends on modified base metrics.

$$MISS = \text{Min}\left(1 - [(1 - \text{CR} \times \text{MC}) \times (1 - \text{IR} \times \text{MI}) \times (1 - \text{AR} \times \text{MA})],\ 0.915\right) \quad (6)$$

$$MI = \begin{cases} 6.42 \times \text{MISS}, & \text{If MS is Unchanged} \\ 7.52 \times (\text{MISS} - 0.029) - 3.25 \times (\text{MISS} \times 0.9731 - 0.02)^{15}, & \text{If MS is changed} \end{cases} \quad (7)$$

$$\text{ME} = 8.22 \times \text{MAV} \times \text{MAC} \times \text{MPR} \times \text{MUI} \quad (8)$$

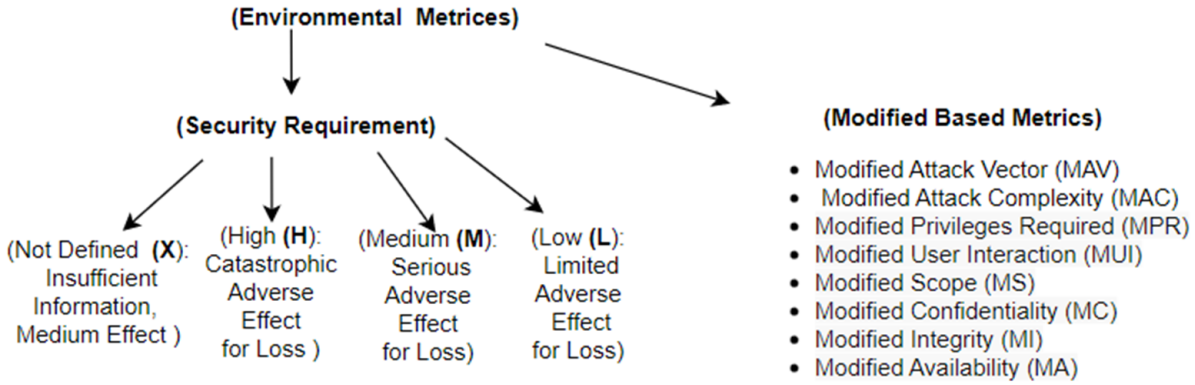

Figure 7. Environmental metric taxonomy (Source: Article authors).

9. Conclusions

This research is a review article that provides extensive study of the penetration testing requirements: frameworks, standards, tools, and scoring methods by which an organization executes perfectly according to its needs. Regular penetration practice will improve the quality of service and the sustainability of an organization by reducing the security risk. This study enhances the scope of the researchers to explore their interest in the latest trend of cyber pen testing processes, tools, and techniques. It also describes the possible vulnerabilities and the domain of penetration testing along with its importance. This study explores the dimensions of penetration testing and execution complexity. This article shows that security is an integrated task, and compromising is not acceptable in either physical or logical infrastructure and platforms (applications, devices, medium, etc.). The rest of this section consists of recent trends in penetration practice, our observations, and the scope of future works.

9.1. Recent Trend

According to the "Cobalt's penetration state 2022" report, the most frequent vulnerabilities happened because of misconfigurations of server security (38%) in 2022, followed by cross-site scripting (13%), access control compromising (11%), sensitive data exploitation (10%), and compromising authentication (8%) [98]. The number of vulnerabilities is increasing day by day, and 66 zero-day vulnerabilities appeared in 2021; 62% of security teams had zero-day exploitation experience in 2022 [22]. On average, 14 days were required for fixing a zero-days attack [98]. The Microsoft 365 suite is utilized by more than one million companies worldwide and creates issues with sensitive data leakage, privilege abuse, and credential theft [99]. DevSecOps, blockchain-centric technologies, cloud services, machine learning, 5-G networks, GRC, SIEM, and helpdesk systems are enhanced in the digital world. New challenges appear within new technologies too. Organizations integrate penetration testing plans into their policy when they are utilizing the aforementioned technologies [100]. AI-centric cybersecurity applications are imposed into network and end devices to improve automatic protection [100], and as a result, automatic pen testing also become popular. An automatic penetration system is more sustainable, but most of the organizations practice manual penetration tests beside AI-centric protection. Table 7 shows the recent contributions to the automatic penetration test that can reduce manual tasks but cannot demolish the importance of manual processes.

Table 7. Recent Penetration trends (Source: Article authors).

Reference	Year	Proposal	Way of Execution Penetration	Limitation
Sanyam et al. [101]	2023	Automated cyber defense	Automated real-time network protection agent generation that would be adaptable for regular penetration testing.	Only for malware penetration.
Faeroy et al. [102]	2023	Autonomous penetration	Proposed a model for autonomous penetration test and focuses on the vulnerabilities identification of IoT devices.	Limited by Wi-Fi vulnerabilities for IoT.
Guewen et al. [103]	2023	Automated building safety	Proposed autonomous three-level security for building an automation system that is applicable for regular penetration.	Limited physical penetration.
Fredrik et al. [104]	2023	Manual pen testing	Applied to a house for physical security and surveillance.	Applied for physical penetration.
Phillip and Saritha [105]	2023	Pen testing Simulation	Applied the reinforcement learning method for simulation-based penetration testing.	For autonomous vehicles.
Massimiliano et al. [106]	2022	Systematic IoT testing	Proposed intelligent thread modeling system for performing penetration on IoT infrastructure.	For home IoT security devices.
Ceren Comenrt et al. [107]	2022	Secure fingureprinting transmission method	Various augmentive methods are applied to securely transmit radio frequency fingerprinting in critical infrastructure such as autonomous vehicle networks.	Only for radio frequency fingureprinting receivers.
O.M Gul et al. [108]	2023	Secure fingureprinting transmission approach	Various augmentive methods are applied to securely transmit radio frequency fingerprinting in critical infrastructure such as industrial IoT.	Only industry IoT environments are considered.
Z. chen et al. [109]	2023	Tempering protection system	A blockchain-based decentralized mobile crowdsensing is proposed, which is against tempering in IoT sensing environments.	Works against tempering and fake requests.

9.2. Observation

Penetration testing services remain some of the critical tasks of an organization's security strategy. Appropriate pen testing programs and equipment are essential to handling security risk proactively. The testing scope and priorities are specified by top security management, which vary from organization to organization. A sufficient security budget can support protecting from threats [100]. An organization is controlled by its internal and external policy procedure, and penetration testing is strongly connected with cybersecurity policy procedures, social and ethical issues, and federal or international laws. It also depends on technology, services, and vendors' responsibility. From this study, we conclude that:

- Integrated penetration policy procedures should be guided by standards and frameworks.
- Organizations should show importance of all vulnerabilities and consider that security is an integrated task (any weakness could be a cause of a massive disaster).
- Organizations should implement the penetration test regularly or on demand (new/updated deployment), which could be both manual and automatic to improve the validation of the test result. The penetration process should be reviewed and updated regularly to protect the system from newly arrived threats.
- Penetration practice minimizes unexpected damages and disruptions; as a result, an organization can ensure quality of service and improve sustainable practices.

9.3. Future Work

Until now, cyber penetration teams have implemented customized risk management methodologies or auditing frameworks, and NIST is the most popular standardization authority. This study conducted a descriptive analysis for frameworks, standards, tools,

and scoring techniques that will be updated by analytical studies in the future. In the future, we are going to propose a specialized penetration framework for demolishing the customizing task of the penetration team. The study finds plenty of open-source tools which are currently used in the penetration process, and Metasploit is one of the most popular in developing payloads that attract our attention. Penetration is a regular activity that is maintained by standard organizations to achieve business goals, and its complexity increases when more functionalities are added to the information system. We can propose a divide-and-conquer technique in the future to minimize its complexity. We have the scope to focus on automation penetration testing for fixed security elements such as intrusion detection systems, intrusion prevention systems, and firewalls. There are plenty of tools that are used for multiple penetration tasks, and a good tool analysis study can guide a penetration team in selecting effective tools. Different technical flaws are being introduced day by day with technological advantages, and new hacking tricks are introduced for cyberattacks. As a result, the penetration demand will increase with new tools and techniques. In the concluding remarks, we want to mention that the study is limited by descriptive analysis, generalized discussions, and broad study domains and is applicable to common platforms. A framework would be developed for a domain such as penetration testing for (i) IoT, (ii) databases, (iii) servers, etc. with a set of selected tools, techniques, methods, and standards.

Author Contributions: K.U.S. is the correspondence and the first author who has conceptualized, developed, and completed the write-up. F.Y. reviewed, cross-checked, and formatted the paper, and A.D. supervised the task and finalized the work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Senol, M.; Karacuha, E. Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *J. Eng.* **2020**, *2020*, 5267564. [CrossRef]
2. Alzoubi, Y.I.; Osmanaj, V.H.; Jaradat, A.; Al-Ahmad, A. Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Secur. Priv.* **2021**, *4*, e145. [CrossRef]
3. Villa, E.; Ruiz, L.; Valencia, A.; Picón, E. Electronic commerce: Factors involved in its adoption from a bibliometric analysis. *J. Theor. Appl. Electron. Commer. Res.* **2018**, *13*, 39–70. [CrossRef]
4. Chukwu, M.A.; Idoko, E.C. Inhibitors of Electronic Banking Platforms' Usage Intention in Deposit Money Banks: Perspectives of Elderly Customers in Developing Economy. *Schizophr. Bull.* **2021**, *7*, 134–145. [CrossRef]
5. Buja, A.G. Cyber Security Featuresfor National E-Learning Policy. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 1729–1735. [CrossRef]
6. Barr, J.R.; D'Auria, D.; Persia, F. Telemedicine, Homecare in the Era of COVID-19 & Beyond. In Proceedings of the Third International Conference on Artificial Intelligence for Industries (AI4I), Irvine, CA, USA, 21–23 September 2020; pp. 48–51.
7. Herrera, A.V.; Ron, M.; Rabadão, C. National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In Proceedings of the 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 21–24 June 2017; pp. 644–648.
8. Robichau, B.P. *Healthcare Information Privacy and Security: Regulatory Compliance and Data Security in the Age of Electronic Health Records*, 1st ed.; 233 Spring St Fl 7; Apress: New York, NY, USA, 2014; ISBN 10-1430266767.
9. Yang, P.; Xiong, N.; Ren, J. Data security and privacy protection for cloud storage: A survey. *IEEE Access* **2020**, *8*, 131723–131740. [CrossRef]
10. Al Jaafreh, A.; Al-Adaileh, R.; Gill, A.; Al-Ani, A.; Alzoubi, Y. A review of literature of initial trust in e-services: The case of internet banking services in Jordanian context. *J. Electron. Bank. Syst.* **2014**, *2014*, 690673. [CrossRef]
11. Alzoubi, Y.I.; Al-Ahmad, A.; Jaradat, A. Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 5081–5088. [CrossRef]

12. UVM. Enterprise Risk Management Program: Guide to Risk Assessment & Response. Available online: https://www.uvm.edu/sites/default/files/Enterprise-Risk-Management/POSTED_Prog_Primer_Trustee_Orientation.pdf (accessed on 10 September 2022).
13. InfoSec Institute. Ashley Madison Revisited: Legal, Business and Security Repercussions. Available online: http://resources.infosecinstitute.com/ashley-madison-revisited-legal-business-and-security-repercussions (accessed on 10 September 2022).
14. PwC. Limiting the Impact of Data Breaches the Case of the Sony Play Station Network. Available online: http://www.strategyand.pwc.com/reports/limiting-impact-data-breaches-case (accessed on 10 September 2022).
15. Dark Reading. Sony Data Breach Cleanup to Cost $171 Million. Available online: http://www.darkreading.com/attacks-and-breaches/sony-data-breach-cleanupto-cost-\protect\T1\textdollar171-million/d/d-id/1097898 (accessed on 10 September 2022).
16. Lee, T. Forget the Ashley Madison or Sony Hacks—A Crippling Cyberattack Is Imminent in the US. The Guardian. Available online: http://www.theguardian.com/technology/2015/jul/26/cybercrime-hacking-internet-of-things-target (accessed on 10 September 2022).
17. The Huffington Post. A Look Back at the Target Breach. Available online: http://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html (accessed on 10 September 2022).
18. Talktalk Hackers Go on £600 Spending Spree with Stolen Card Details as Boss Says Its too Early to Consider Compensation. The Mirror. Available online: http://www.mirror.co.uk/news/uk-news/talktalk-hackers-go-600-spending6694321 (accessed on 10 September 2022).
19. Ashley, M. Aftermath: Confessions, Suicide Reports and Hot on the Hacker's Trail. National Post. Available online: http://news.nationalpost.com/news/canada/ashley-madison-aftermath-confessions-suicide-reports-and-hot-on-the-hackers-trail (accessed on 10 September 2022).
20. McDaid, L. Talktalk Cyber-Attack: County Londonderry Man Targeted. BBC News. Available online: http://www.bbc.co.uk/news/uk-34613921 (accessed on 10 September 2022).
21. Pranggono, B.; Arabo, A. COVID-19 pandemic cybersecurity issues. *Internet Technol. Lett.* **2020**, *4*, e247. [CrossRef]
22. Rijnetu, I. 100+ Essential Penetration Testing Statistics [2023 Edition], Pentest. Publisher Pentest-Tools.com. February 2023. Available online: https://pentest-tools.com/blog/penetration-testing-statistics (accessed on 16 April 2023).
23. Shank, S. Penetration Testing in 2022: Key Trends and Challenges. The State of Security. Available online: https://www.tripwire.com/state-of-security/security-data-protection/penetration-testing-in-2022-key-trends-and-challenges/ (accessed on 20 September 2022).
24. Recent Cyber Attacks & Data Breaches in 2022. Available online: https://purplesec.us/security-insights/data-breaches/ (accessed on 19 September 2022).
25. Perwej, Y.; Abbas, Q.; Dixit, J.P.; Akhtar, N.; Jaiswal, A.K. A Systematic Literature Review on the Cyber Security. *Int. J. Sci. Res. Manag.* **2021**, *9*, 669–710. [CrossRef]
26. Goel, J.N.; Mehtre, B.M. Vulnerability assessment & penetration testing as a cyber-defense technology. *Procedia Comput. Sci.* **2015**, *57*, 710–715. [CrossRef]
27. Ghanem, C.; Chen, T.M. Reinforcement learning for efficient network penetration testing. *Inf. Int. Interdiscip. J.* **2020**, *11*, 6. [CrossRef]
28. Vaca, A.J.V.; Gasca, R.M.; Fombella, J.A.C.; Lopez, M.T.G. AMADEUS: Towards the Automated security testing. In Proceedings of the 24th ACM Conference on Systems and Software Product Line: Volume A, New York, NY, USA, 19–23 October 2020; pp. 1–12.
29. Yaacoub, J.P.; Hassan, N.; Noura, O.S.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **2021**, *15*, 115–158. [CrossRef] [PubMed]
30. Nguyen, G.; Dlugolinsky, S.; Tran, V.; Garcia, A.L. Deep learning for proactive network monitoring and security protection. *IEEE Access* **2020**, *8*, 19696–19716. [CrossRef]
31. Trifonov, R.; Manolov, G.; Yoshinov, R.; Pavlova, G. A Survey of Artificial Intelligence for Enhancing the Information Security. *Int. J. Dev. Res.* **2017**, *7*, 16866–16872. Available online: https://www.journalijdr.com/sites/default/files/issue-pdf/10933.pdf (accessed on 12 October 2022).
32. Collier, Z.; DiMase, D.; Walters, S.; Tehranipoor, M.; Lambert, J. Cybersecurity Standards: Managing Risk and Creating Resilience. *Computer* **2014**, *47*, 70–76. [CrossRef]
33. Knapp, K.J.; Maurer, C.; Plachkinova, M. Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *J. Inf. Syst. Educ.* **2017**, *28*, 101–114.
34. CVE Details, The Ultimate Security Vulnerability Datasource. Available online: https://www.cvedetails.com/vulnerability-list/year-2023/vulnerabilities.html (accessed on 4 June 2023).
35. Sarker, K.U.; Deraman, A.; Hasan, R.; Abbas, A. A 4-Layered Plan-driven Model (4LPdM) to Improve Software Development. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2022**, *13*, 589–600. [CrossRef]
36. Sarker, K.U.; Deraman, A.; Hasan, R.; Abbas, A. SQ-Framework for Improving Sustainability and Quality into Software Product and Process. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2020**, *11*, 69–78. [CrossRef]
37. Herzog, P. *The Open Source Security Testing Methodology Manual (OSSTMM) 3. Contemporary Security Testing and Analysis*; ISECOM: Cardedeu, Spain, 2010.

38. Saad, E.; Mitchel, R. OWASP Web Security Testing Guide, Version 4.2. OSASP. Available online: https://owasp.org/www-project-web-security-testing-guide/ (accessed on 17 March 2023).
39. Willemsen, J.; Holguera, C.; Mueller, B.; Schleier, S. MASTG. Mobile Application Security Testing Guide. Version v1.5.0. Available online: https://mas.owasp.org/#our-mission (accessed on 17 March 2023).
40. OWASP Firmware Security Testing Methodology. Available online: https://github.com/scriptingxss/owasp-fstm (accessed on 22 September 2022).
41. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 17 March 2023).
42. PTEST. High Level Organization of the Standard. Available online: http://www.pentest-standard.org/index.php/Main_Page (accessed on 23 March 2023).
43. PTES Technical Guidelines. Available online: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (accessed on 23 September 2022).
44. FAQ. Penetration Testing Execution Standard. Available online: http://www.pentest-standard.org/index.php/FAQ (accessed on 23 March 2023).
45. Information System Security Assessment Framework (ISSAF). Future Learn. Available online: https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521 (accessed on 23 March 2023).
46. Cordero, J.A.V. ISO/IEC standards as mechanisms of proactive responsibility in the General Data Protection Regulation. *Internet Derecho Política Rev. D'internet Dret Política* **2021**, *33*, 7.
47. Arora, V. *Comparing Different Information Security Standards: COBIT vs. ISO 27001*; Carnegie Mellon University: Doha, Qatar, 2010. Available online: https://varunarora.com/assets/iso27001-vs-cobit/paper.pdf (accessed on 3 April 2023).
48. Boboň, S. *Analysis of NIST FIPS 140-2 Security Certificates*; Masaryk University: Brno, Czech Republic, 2021. Available online: https://is.muni.cz/th/wftuc/?lang=en (accessed on 12 April 2023).
49. Azmi, R.; Tibben, W.; Win, K. Review of cybersecurity frameworks: Context and shared concepts. *J. Cyber Policy* **2018**, *3*, 258–283. [CrossRef]
50. Huamani, R.; Eduardo, R. *Implementación de un Plan de Seguridad Informática Basado en la Norma ISO IEC/27002, Para Optimizar la Gestión en la Corte Superior de Justicia de Lima*; Universidad Privada del Norte: Trujillo, Peru, 2022. Available online: https://hdl.handle.net/11537/29848 (accessed on 13 April 2023).
51. Putri, M.K.; Hakim, A.R. Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO/IEC 27005: 2018 dan NIST SP 800-30 Revisi 1. *J. Info Kripto* **2021**, *15*, 134–141. [CrossRef]
52. Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics* **2022**, *11*, 2181. [CrossRef]
53. Choo, K.-K.R.; Gai, K.; Chiaraviglio, L.; Yang, Q. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Comput. Secur.* **2021**, *102*, 102136. [CrossRef]
54. Macher, G.; Schmittner, C.; Veledar, O.; Brenner, E. ISO/SAE DIS 21434 Automotive Cybersecurity Standard—In a Nutshell. In *Computer Safety, Reliability, and Security*; Springer: Cham, Switzerland, 2020; Volume 12235, pp. 123–135. [CrossRef]
55. Leander, B.; Čaušević, A.; Hansson, H. Applicability of the IEC 62443 Standard in Industry 4.0/IIoT. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26 August 2019; Association for Computing Machinery: New York, NY, USA; Canterbury, UK, 2019; pp. 1–8.
56. Tofan, D. Information Security Standards. *J. Mob. Embed. Distrib. Syst.* **2011**, *3*, 128–135.
57. Schmitz, C.; Schmid, M.; Harborth, D.; Pape, S. Maturity level assessments of information security controls: An empirical analysis of practitioners' assessment capabilities. *Comput. Secur.* **2021**, *108*, 102306. [CrossRef]
58. Basu, S. 17 Best Penetration Testing Tools/Software of 2022 [Reviewed], Astra Security Blog. 2022. Available online: https://www.getastra.com/blog/security-audit/best-penetration-testing-tools/?utm_term=&utm_campaign (accessed on 15 April 2023).
59. Fruhlinger, J.; Porup, J.M. 11 Penetration Testing Tools the Pros Use, CSO Online. CSO. Available online: https://www.csoonline.com/article/2943524/11-penetration-testing-tools-the-pros-use.html (accessed on 15 April 2023).
60. Siyal, G. The Top 10 Penetration Testing Tools for Security Professionals, MUO. Available online: https://www.makeuseof.com/penetration-testing-for-security-professionals/ (accessed on 15 April 2023).
61. Jevtic, G. 13 Powerful Penetration Testing Tools the Pros Use, phoenixNAP Blog. Available online: https://phoenixnap.com/blog/best-penetration-testing-tools (accessed on 15 April 2023).
62. Williams, L. 27 Best Penetration Testing (Pentest) Tools in 2022, Guru99. Available online: https://www.guru99.com/top-5-penetration-testing-tools.html (accessed on 15 April 2023).
63. Editorial, G. Astra Pentest Reviewed—Easy, Continuous Vulnerability Scanning & Compliance, Geekflare. Available online: https://geekflare.com/astra-pentest-review/ (accessed on 15 April 2023).
64. Risk Scoring System. Characterizing Identified Vulnerabilities and Numerically Scoring the Potential Severity Using a Mission Impact Focus. Available online: https://www.riskscoringsystem.com/ (accessed on 13 April 2023).
65. INCIBE. Industrial CVSS: Alternative Calculations for Different Needs. 2019. Available online: https://www.incibe-cert.es/en/blog/industrial-cvss-alternative-calculations-different-needs (accessed on 13 April 2023).

66. Bodungen, C. Industrial Vulnerability Scoring System (IVSS). 2019. Available online: https://securingics.com/IVSS/IVSS.html (accessed on 15 April 2023).
67. Figueroa-Lorenzo, S.; Añorga, J.; Arrizabalaga, S. A Survey of IIoT Protocols. *ACM Comput. Surv.* **2020**, *53*, 1–53. [CrossRef]
68. Strategies to Mitigate Cyber Security Incidents—Mitigation Details. Australian Signals Directorate, Australian Cyber Security Centre. February 2017. Available online: www.cyber.gov.au/sites/default/files/2019-03/Mitigation_Strategies_2017_Details_0.pdf (accessed on 15 April 2023).
69. CVSS Version 3.1 Release. Common Vulnerability Scoring System Version 3.1: Specification Document. Available online: https://www.first.org/cvss/specification-document (accessed on 15 April 2023).
70. Al-Ahmad, A.S.; Kahtan, H.; Hujainah, F.; Jalab, H.A. Systematic literature review on penetration testing for mobile cloud computing applications. *IEEE Access* **2019**, *7*, 173524–173540. [CrossRef]
71. Alghamdi, A.A. Effective Penetration Testing Report Writing. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, 7–8 October 2021; pp. 1–5.
72. Singh, A. *Metasploit Penetration Testing Cookbook*, 2nd ed.; Packt Publishing: Birmingham, UK, 2012; ISBN 978-1849517423.
73. Moradov, O. Penetration Testing Report: 6 Key Sections and 4 Best Practices. 2021. Available online: https://brightsec.com/blog/penetration-testing-report/ (accessed on 18 September 2022).
74. Caudill, B. Four Things Every Penetration Test Report Should Have. Available online: https://rhinosecuritylabs.com/penetration-testing/four-things-every-penetration-test-report/ (accessed on 18 September 2022).
75. Firewall Penetration Testing: Steps, Methods & Tools. Available online: https://purplesec.us/firewall-penetration-testing/ (accessed on 19 September 2022).
76. 2022 Penetration Testing Report. Coresecurity by HelpSystem. Available online: https://static.helpsystems.com/core-security/pdfs/guides/cs-2022-pen-testing-report.pdf (accessed on 15 September 2022).
77. Paul, G.; Irvine, J. Privacy implications of wearable health devices. In Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, UK, 9–11 September 2014; pp. 117–121.
78. Herzig, T.; Walsh, T. *Implementing Information Security in Healthcare: Building a Security Program*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2020; ISBN 978-1938904349.
79. Li, R.; Zhao, Z.; Sun, Q.; Chih-Lin, I.; Yang, C.; Chen, X.; Zhao, M.; Zhang, H. Deep reinforcement learning for resource management in network slicing. *IEEE Access* **2018**, *6*, 74429–74441. [CrossRef]
80. Houser, A.M. Mental Models for Cybersecurity: A Formal Methods Approach. University at Buffalo, State University of New York. 2018. Available online: http://fhsl.eng.buffalo.edu/publications/Houser_dissertation.pdf (accessed on 13 April 2023).
81. Kostyuk, N.; Wayne, C. Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats. Available online: http://www-personal.umich.edu/~nadiya/communicatingcybersecurity.pdf (accessed on 13 April 2023).
82. Jump, M. Fighting Cyberthreats with Technology Solutions. *Biomed. Instrum. Technol.* **2019**, *53*, 38–43. [CrossRef]
83. Jain, A.K.; Goel, D.; Agarwal, S.; Singh, Y.; Bajaj, G. Predicting Spam Messages Using Back Propagation Neural Network. *Wirel. Pers. Commun.* **2020**, *110*, 403–422. [CrossRef]
84. Farahmand, F.; Navathe, S.B.; Enslow, P.H.; Sharp, G.P. Managing vulnerabilities of information systems to security incidents. In Proceedings of the 5th International Conference on Electronic Commerce, Pittsburgh, PA, USA, 30 September–3 October 2003; Association for Computing Machinery: New York, NY, USA; pp. 348–354.
85. Perwej, Y.; Omer, M.K.; Sheta, O.E.; Harb, H.A.M.; Adrees, M.S. The Future of Internet of Things (IoT) and Its Empowering Technology. *Int. J. Eng. Sci. Comput. (IJESC)* **2019**, *9*, 20192–20202.
86. Xiao, B.; Chen, W.; He, Y.; Hsing, E.; Sha, M. An Active Detecting Method against SYN Flooding attack. In Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS2005), Fukuoka, Japan, 20–22 July 2005; pp. 709–715.
87. Keshri, A. Top 5 Penetration Testing Methodologies and Standards. 2022. Available online: https://www.getastra.com/blog/security-audit/penetration-testing-methodology/#owasp (accessed on 23 March 2023).
88. Bertoglio, D.D.; Zorzo, A.F. Overview and open issues on penetration test. *J. Braz. Comput. Soc.* **2017**, *23*, 2. [CrossRef]
89. Insight Report. Global Cybersecurity Outlook. WorForum. January 2022. Available online: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (accessed on 25 March 2023).
90. Purser, S. Standards for Cyber Security. In *Best Practices in Computer Network Defense: Incident Detection and Response*; Hathaway, M.E., Ed.; IOS Press: Washington, DC, USA, 2014; pp. 97–106. ISBN 978-1614993711.
91. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access* **2021**, *9*, 121975–121995. [CrossRef]
92. Taherdoost, H. Understanding of E-service Security Dimensions and its effect on Quality and Intention to Use. *Inf. Comput. Secur.* **2017**, *25*, 535–559. [CrossRef]
93. Maleh, Y.; Sahid, A.; Alazab, M.; Belaissaoui, M. *IT Governance and Information Security: Guides, Standards, and Frameworks*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2021; ISBN 9780367753245.
94. Fonseca-Herrera, O.A.; Rojas, A.E.; Florez, H. A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci.* **2021**, *48*, 213–222. Available online: https://www.iaeng.org/IJCS/issues_v48/issue_2/IJCS_48_2_01.pdf (accessed on 12 April 2023).

95. Arora, D. Five Penetration Testing Challenges that Should Concern Organizations. ERMProtect IT Security Consultant. Available online: https://ermprotect.com/blog/five-penetration-testing-challenges-that-should-concern-organizations/ (accessed on 13 April 2023).
96. Dong, S.; Cao, J.; Fan, Z. A Review on Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards. Available online: https://arxiv.org/ftp/arxiv/papers/2108/2108.08089.pdf (accessed on 1 April 2023).
97. Mell, P.; Scarfone, K.; Romanosky, S. CVSS v2 Complete Documentation. FIRST. Available online: www.first.org/cvss/v2/guide (accessed on 13 April 2023).
98. Paz, J. The State of Pen Testing 2022 Report, Cobalt. Available online: https://www.cobalt.io/blog/the-state-of-pentesting-2022-how-labor-shortages-are-impacting-cybersecurity-and-developer-professionals (accessed on 15 April 2023).
99. Chopra, S. The Ultimate Checklist for Your Penetration Testing Report. 26 May 2023. Available online: https://redfoxsec.com/blog/penetration-testing-report/ (accessed on 12 June 2023).
100. Penetration Testing: Trends & Challenges in 2022: Valuementor. Cyber Security Services & Payment Security Services Company. Available online: https://valuementor.com/penetration-testing/penetration-testing-trends-challenges-in-2022/ (accessed on 16 April 2023).
101. Vyas, S.; Hannay, J.; Bolton, A.; Burnap, P. Automated Cyber Defence: A Review. *Proc. ACM Meas. Anal. Comput. Syst.* **2023**, *37*, 111.
102. Faeroy, F.L.; Yamin, M.M.; Shukla, A.; Katt, B. Automatic Verification and Execution of Cyber Attack on IoT Devices. *Sensors* **2023**, *23*, 733. [CrossRef]
103. Li, G.; Ren, L.; Fu, Y.; Yang, Z.; Adetola, V.; Wen, J.; Zhu, Q.; Wu, T.; Candan, K.S.; O'Neill, Z. A critical review of cyber-physical security for building automation systems. *Annu. Rev. Control* **2023**, *55*, 237–254. [CrossRef]
104. Heiding, F.; Süren, E.; Olegård, J.; Lagerström, R. Penetration testing of connected households. *Comput. Secur.* **2023**, *126*, 103067. [CrossRef]
105. Garrad, P.; Unnikrishnan, S. Reinforcement learning in VANET penetration testing. *Results Eng.* **2023**, *17*, 100970. [CrossRef]
106. Rak, M.; Salzillo, G.; Granata, D. ESSecA: An automated expert system for threat modelling and penetration testing for IoT ecosystems. *Comput. Electr. Eng.* **2022**, *99*, 107721. [CrossRef]
107. Comert, C.; Kulhandjian, M.; Gul, O.M.; Touazi, A.; Ellement, C.; Kantarci, B.; D'Amours, C. Analysis of Augmentation Methods for RF Fingerprinting under Impaired Channels. In Proceedings of the 2022, ACM Workshop on Wireless Security and Machine Learning (WiseML'22), San Antonio, TX, USA, 19 May 2022; Association for Computing Machinery: New York, NY, USA; pp. 3–8. [CrossRef]
108. Gul, O.M.; Kulhandjian, M.; Kantarci, B.; Touazi, A.; Ellement, C.; D'amours, C. Secure Industrial IoT Systems via RF Fingerprinting Under Impaired Channels with Interference and Noise. *IEEE Access* **2023**, *11*, 26289–26307. [CrossRef]
109. Zhiyan, C.; Omer, M.G.; Burak, K. Practical Byzantine Fault Tolerance-based Robustness for Mobile Crowdsensing. *Distrib. Ledger Technol.* **2023**, *2*, 2769–6472. [CrossRef]