

Efficacy of Unconventional Penetration Testing Practices

Bandar Abdulrhman Bin Arfaj¹, Shailendra Mishra^{2,*} and Mohammed Alshehri¹

¹Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia

²Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia

*Corresponding Author: Shailendra Mishra. Email: s.mishra@mu.edu.sa

Received: 14 April 2021; Accepted: 15 May 2021

Abstract: The financial and confidential cost of cyberattack has presented a significant loss to the organization and government where the privacy of worthless information has become vulnerable to cyber threat. In terms of efforts implemented to avoid this risk, the cyberattack continues to evolve, making the cybersecurity systems weekend. This has necessitated the importance of comprehensive penetration testing, assessment techniques, and tools to analyze and present the currently available unconventional penetration techniques and tactics to test and examine their key features and role in supporting cybersecurity and measure their effectiveness. The importance of cyberspace and its value make it an eminent target for attackers to exploit any vulnerability they may encounter in the respective system. Due to the cybersecurity risks, robust security measures need to be put in place to protect the system in question. Penetration testing is one such security measure that aims to uncover the security vulnerabilities in the system. Due to the dynamic aspect of cyberspace and technology, advanced or more unusual penetration testing mechanisms need to be employed to deal with the emerging vulnerabilities and security threats in cyberspace. This research explores and utilizes the conventional and unconventional penetration testing methods and identifies the study's main objectives to improve the current penetration testing techniques to increase security effectiveness and efficiency. It also calculates vulnerabilities and risks based on Common Vulnerability Scoring System (CVSS) scores and their impact on confidentiality, integrity, and availability. It proposes a Wi-Fi penetration testing approach based on Kali Linux. It also highlights the conventional and unconventional penetration testing approaches and justifies the essence of penetration testing over cyberattack cases. Due to the dynamic changes in technology, the conventional penetration testing method does not seem to be efficient to achieve its goal.

Keywords: Vulnerability; threat; cyber-attack; penetration testing



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

Cyber information is considered a highly valued asset in business and government organizations that require secure systems to protect against cyber-attacks in the era of great economic and knowledge competition. Despite implementing a security system, cyber information is still at risk of hacking, and the organization's business information can be leaked and exposed [1]. Subsequently, the security breach damages the company's reputation and leads to loss of investment opportunities and shareholders as trust in the company is lost [2]. Government policies have been established to organize the process of securing personal and organizational data and prevent data leakage. Legal agreements and international standards have been applied to protect their rights.

Nevertheless, companies and government institutions usually rely on outsourcing companies to regulate the organization's cybersecurity operations. However, these companies require evaluating their services and their effectiveness, which involves applying metrics to assess the benefits. Ordinary metrics that evaluate the ordinary internet cannot measure cybersecurity, so specific metrics should be provided to facilitate reporting on the states of cybersecurity operations [3]. As for the security and protection of this information, requires working on implementing systems, developing software specialized in countering hacking and espionage, and strengthening electronic protection systems.

Although the techniques used in penetration and violation of the privacy of important information for organizations and banks result in a great financial and material loss, it was necessary to continuously update these systems to ensure that cyber-attacks are fully and efficiently resisted, and develop and provide unconventional anti-techniques and tools to combat cyber-attacks [4,5]. The Key Performance Measures of cybersecurity operations center in government agencies or private companies include quality, time, and cost, under the three stakeholder metrics: organizational, operational, and external. Therefore, some required metrics should be determined by the organization.

The metrics should be expressed according to the interests of each audience. Measuring cost can be a hindrance in cyber assurance operations; fixed resources can be priced, besides end-user satisfaction can be estimated [6]. Business in the world is moving towards implementing digital and automated systems and tools. Yet, implementing this advanced technology makes the organization vulnerable to cyber-attacks — standardized policies provided for risk assessment and change in the network and systems. A critical phase in assessing the threat of intrusion is quantifying and measuring the network's vulnerability or subscribers.

Since various scoring systems are available in the cybersecurity domain, the Common Vulnerability Scoring System (CVSS) stands out for its advantage in determining the baseline score for various objects and the ability to obtain a customizable score [7,8]. The principle of penetration testing is to perform an attempted attack on the cybersecurity system to evaluate the measures and effectiveness of the security system designed to protect the information system. Penetration testing may be conducted as part of a newly implemented system before final management approval or frequent security assessment when major updates have been made as part of the operational system [9,10].

This research targets the increasing vulnerabilities in wireless network communication. This research proposed a Wi-Fi penetration testing approach based on Kali Linux. Kali Linux has a positive effect in improving the security assessment of a given wireless communication-based computer system. There are four main phases in the proposed approach: preparation, information gathering, attack simulation and reporting. The proposed approach in this research also involves using password monitoring, scanning, capturing, analyzing, and cracking techniques. Penetration testing is generally used to identify security vulnerabilities that may exist in a system.

The test usually involves simulating numerous security attacks on the target system. In this research, automated security evaluation has been proposed to evaluate the security status of a given computer system using automated tools and techniques. This generally aims to reduce the cost and time of

penetration testing, thus motivating users to perform the test frequently. In this case, the potential risk of a cyber-attack is anticipated and assessed. Penetration testing can be applied in many areas, including operational, technical, or administrative. The conventional techniques have relied on modifying the security system to face and deal with the available cyber-attacks to avoid the damage and loss resulting from illegal access to the organization's information and data.

The traditional techniques have specific characteristics that are considered common to an effective security system. These characteristics include quick response, cost-effectiveness, time-oriented and repairable [11,12]. Considering these characteristics, the traditional cybersecurity system has exposed large companies and organizations, and governments to the risk of cyber-attacks. This situation required the implementation of effective techniques and tools that unconventionally test and predict the penetration of cyber-attacks into the networks [13]. Over the years, cyberspace has witnessed several severe attacks that have crippled digital services and caused massive losses to the respective businesses. The risk-based security report shows that there has been an enormous increase in cyber-attacks over the last decade. According to this report, a whopping 284 percent increase in sensitive information is compromised in cyberspaces [14].

The Yahoo case of 2013 still stands as the largest attack that led to the compromise of nearly 3 billion Yahoo accounts. This is just the tip of the iceberg of known cyber-attacks that have occurred in the recent past [15]. They are predicted to increase as more devices are added to cyberspace. Nowadays, there are so many evolved cyber threats and attacks. For example, a decade ago, the denial of service attack was the well-known common attack that “denied services to system users,” today, it has evolved into a distributed form of denial of service attack. In this form of attack, packets or requests are flooded from multiple sources, making it difficult to control. Security has evolved from the normal security measures to sophisticated security measures including various penetration tactics discussed in this research. This can be considered as a direct proportionality relationship that is a result of technological development.

Previous authors [16,17] mainly focus on the continuous review and modification of the cybersecurity system. Regardless of the importance of the review, the process is considered costly and monotonous. The study reported in [18] classifies the phases of penetration testing into the pre-attack phase with passive exploration and active exploration. The method discussed in [19] uses the software product line to explore the vulnerabilities of the system configuration. This research is a step toward exploring conventional and unconventional penetration testing over cyber-attack cases to increase security effectiveness. It also finds a way to calculate vulnerabilities and risks based on CVSS scores. Conventional penetration testing is not suitable in today's world due to dynamic changes. In this research, a virtual environment was set up, and IPs and devices were exploited using Kali Linux Tools, and the experiment was conducted for digital forensics. In the virtual environment, a web browser is exploited, a forensic investigation of the web browser is conducted to extract the evidence from the browser.

The purpose of this research is also to give comprehensive research on unconventional penetration testing tactics and techniques. This is intended to be achieved by answering the following questions;

- What are the common penetration testing techniques and tactics?
- What are the current statistics in the cyber-attacks?
- What are the trends in cyber-attacks and cyber-security?
- How can the emerging trends of cyber-attacks be addressed?

The first question would elaborate on the commonly used penetration testing tactics and techniques concerning the trends in cyber-security and threats according to the computing regulations worldwide. The second question has its objective of establishing the recent statistics in the cyber-security field to justify the frantic efforts to develop advanced security measures to match the growing vulnerabilities.

Setting the trends in the changes in the entire cyberspace is key to design appropriate penetration testing techniques. This is intended to be achieved by answering the question. Modern computer security problems require modern solutions; this is addressed in question 4 as its objective is to discuss the ever-changing cyber-space.

The main contributions of this research are summarized as follows:

- This research explores and identifies the conventional and unconventional ways of penetration testing.
- This research set up a virtual environment and exploited IPs and devices with Kali Linux Tools, and conducted the experiment for digital forensics investigation.
- The research identifies the main objectives of the research in the efforts to improve the current penetration testing techniques to improve the security effectiveness and its efficiency.
- Compute vulnerabilities and risk based on CVSS scores and their impact on confidentiality, integrity, and availability for automated tests.
- To highlight the conventional and unconventional penetration testing approaches and justify the essence of penetration testing concerning the cyber-attack cases. Due to the dynamic changes in technology, the conventional type of penetration testing seems to be no longer efficient in achieving its goal.

The non-conventional penetration testing methods assume a whole new dimension of automation, from scanning to the re-testing phase of the process. The manual/conventional methods of penetration testing require resources and time to be performed. Due to these requirements, conventional penetration testing is very costly and time-consuming, so it is not optimal in the current business environment. Currently, cyberspace is experiencing massive growth in valuable information and growing concerns about security vulnerabilities. Therefore, calls for automated or more unconventional types of penetration testing.

The rest of this paper is organized as follows. Related works in vulnerabilities, threats, cyber-attacks, penetration testing and countermeasures are discussed in Section 2. The research methodology is presented in Section 3. A detailed discussion of implementation and result analysis is discussed in Section 4. Finally, Section 5 concludes the paper by giving some of the future directions.

2 Literature Review

The most current data sources and published articles and studies dealing with cyber-attack and penetration testing techniques will be explored and discussed to provide a theoretical background and conceptual framework for this research. This study covers cyber-attack and penetration testing, the concept of system vulnerabilities, and their impact on evaluating penetration testing techniques. The principle and standards controlling penetration testing will be reviewed and disclosed to determine the relationship to system and network vulnerabilities. By reviewing the related studies presented below, the objectives and goals of the study are achieved and interpreted scientifically. Organizations spend huge budgets on preventing cyber-attacks and unauthorized access to their data, which costs the organizations and excessive government losses and affects their business. Globally, cyber-attacks are estimated to cost \$600 billion, while they are expected to cost six trillion USD every year.

This attitude requires advanced and unconventional tools to assess and secure the system defending it against cyber-attacks. Therefore, invasive techniques have been implemented to facilitate the evaluation of various situations of security against cyber-attacks [20]. Commonly known conventional techniques for penetration testing can detect and explore the network's vulnerability to attacks. However, some techniques are based on measuring the system's vulnerability to cyber-attacks by simulating an actual

cyber-attack on the network so that the demonstrated steps can be predicted and avoided. In [4,21], the authors proposed accurate teaming methods that emphasize the qualified performance of the security assessment.

However, the automatic stimulation of actual cyber-attacks presents a difficult task in determining the order of the attacker's response. An attack graph is a tool that can be used to show the potential sequence of actions that attackers are likely to perform. The attack graph depends on network vulnerability analysis to provide a group of attack opportunities that do not indicate the attacker's main strategy. However, the attack graph is exponentially complex due to the large size of the current network, leading to scalability issues. Private companies specializing in cybersecurity, in particular, play an essential role in cybersecurity by supporting their clients' technological infrastructure and information with the tools and capabilities necessary to defend against cyberattacks. Governments and organizations trust cybersecurity firms with high confidence and spend a high financial budget to ensure the preservation and protection of sensitive and private information. Their deep investigation into their clients' system information has given them good chances to form an overall understanding of the nature of cyber attackers and their threats [16]. Private cybersecurity firms rely on assessing their cybersecurity performance through the application of penetration testing. However, these firms face some complexities related to clients and their involvement in cyber-attacks. The process of initiating a secure system has successive phases of continuous improvement and evaluation of the system due to the lack of resources and complexity. Failures and conflicts are expected during the operation of the system. Penetration testing is considered ethical hackers who regularly assess the security of the cyber system to reduce the risk of cyber-attacks [1]. The tools used in penetration testing are implemented by specialists. The result of the process results in reporters that include a list of security-related data and the range of its severity and techniques used in producing this data. According to the study reported in [17,18], governments and organizations face various cyber-attacks daily, highlighting the need for constant review and modification of the cybersecurity system. Regardless of the importance of audit, the process is considered costly and monotonous.

The study reported in [19] classifies the phases of penetration testing into the pre-attack phase includes passive exploration and active exploration. The attack phase includes perimeter penetration, target acquisition, privilege escalation, and execution, implantation, and withdrawal. Finally, in the Post-Attack phase, an essential step in penetration testing, where the tester is responsible for restoring the system to its previous situation. To ensure a secure network and data transition, it is essential to implement the appropriate system configuration to prevent the risk of cyber-attack. Assessing the vulnerabilities of the cybersecurity system and its exposure to cyberattacks has become a mandatory task. However, the scope of data and system configuration that is vulnerable is enormous and diverse, making it difficult to cover and mitigate [22].

The method proposed in [19] uses the software product line in exploring the vulnerabilities of the system configuration. Based on a functional model, Automated security testing (AMADEUS) can automatically analyze and test the cybersecurity vulnerabilities, which can detect and identify the cyber threat in the organization's infrastructure. AMADEUS can enhance and support deep security vulnerability detection according to the system configuration that attackers might target. By performing an integrated security compatibility test that AMADEUS performs within a given situation, the attack vector is spontaneously explored. This technique can be considered a structure to detect and investigate the configuration vulnerability within the information system, where it can be used in the reconnaissance phase in penetration testing. In this process, the AMADEUS structure can collect and analyze the appropriate data to be stored in a vulnerability database to predict cyber-attack scenarios.

The principle of traditional techniques used by penetration testing engineers and specialists depends on tracking and observing vulnerabilities in the network to avoid being discovered by others; this method has

proven to be very operational infrequent incidents. Nevertheless, traditional penetration testing techniques are characterized by restrictive rules that prevent the penetration testing process from crossing the ethical boundary. These restrictive codes represent a lack of conservative constraints in the attack patterns that can be used, defining the system boundary, the temporal limits of the mission, and the political and security matters associated with the project, which can form an obstacle that must be avoided [23].

To correctly identify the risk of cyber-attack on the network or system, the defender should leave the social standards and code of ethics to unconventional and radical to identify the attack vector. Otherwise, the tactics of penetration testing will become routine, boring, and useless [24]. The concept of black-hat and white-hat attackers is better explained by the perception of authority. Where one team has no authority to use and access or abuse the data resources. Whereas the other team is authorized to access and explore the data without any restriction. When expert engineers apply an attack within a defined process scope, which may be exceptionally limited, several penetration tools may be omitted [25].

Furthermore, the potential risk that could threaten the organization can be absorbed; thus, the owner can see the drawback of limiting the penetration process. The main obstacles and factors affecting cybersecurity. Identification, preparation, isolation, processing, verification, and report presentation. Cyberspace is continually growing, with more and more devices being added every day. This is a positive trajectory towards the digitization of the world and the economy at large. The digitization results are eminent in every field, such as the medical field, business, security, and general social communication. However, the growth of cyberspace comes with numerous security flaws that need to be taken care of. Penetration testing comes in at this stage as a security measure to evaluate the security status of the respective computer systems. While it is important to evaluate the existing security of computer systems, it is also important to employ more strategic evaluation techniques, tools, and tactics to attain optimal results. The conventional ways of penetration testing involve the manual means of evaluating the computer security of a system. This is effective but less efficient in terms of resource utilization. A delay in identifying a security vulnerability can be costly, resulting in massive impacts on the respective system owners. As will be elaborated in the research objectives, manual penetration testing has not been a cost-effective process; thus, the importance of the unconventional tactics, techniques, and tools in penetration testing is discussed in this research study.

3 Research Methodology

Research methodology is an integral part of research that describes the research framework. This research has theoretical and statistical aspects, so it is conclusive to say that the investigation is mixed. The qualitative aspects of the research focus on the literature of the different penetration testing techniques used conventionally and unconventionally. This may be required for illustration in the form of calculations and programming and thus represents quantitative research. Also, starting from a general point of view of penetration testing, it is conclusive to say that the investigation is deductive and aims to discuss the unconventional type(s) of penetration testing and present it as a solution to the current gap in the conventional types of security evaluation. The idea is to choose a comprehensive research methodology that can cover all aspects of the research.

From the background, it is projected that the research may require some mathematical and program illustrations, hence the choice for a quantitative type. The qualitative aspect of the research is evident in the theoretical aspects of the research, where there are detailed explanations of the research findings. The explanations start with a general view of what is known, hence a deductive type of research. In this regard, a deductive mixed research type is considered more appropriate for this research due to the nature of the research and the expected results in the analysis part. All testing is done as per the National Institute of Standards and Technology Special Publication (NIST SP 800-115) technical guide to

information security testing and assessment [26] in phase wise manner; Conventional penetration testing techniques are more manual techniques that involve tedious tasks, especially writing code to execute the emulated security attacks. Conventional and non-conventional penetration testing use similar procedures and steps in performing security evaluation. These include the various phases of penetration testing, as described below and shown in Fig. 1.

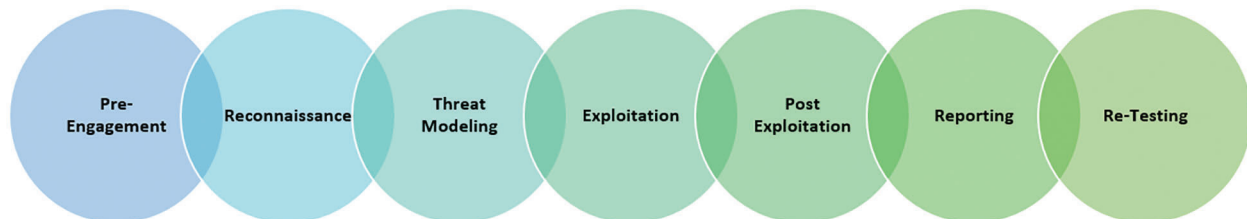


Figure 1: Penetration testing phases

The first phase is the planning/preparation phase, where the goals are defined, and the rules are set. This is about getting an overview of what test the tester wants to do. It is not detailed, but it gives an insight into the target system to be attacked. The reconnaissance phase of penetration testing used to gather intelligent information about the system is the second phase. The third phase is Threat Modeling, scanning/detecting security vulnerabilities are identified. This involves a clear investigation of the identified vulnerabilities and careful elaboration of the possible vulnerabilities that could be executed against the system. The exploitation phase of penetration testing is related to threat modeling, with both being performed in the same step. It is the actual implementation of the emulated security attack in the system. It is the actual implementation of the emulated security attack in the system.

The post-exploitation phase of penetration testing focuses on analyzing the impact of the penetration test. This is where things like CVSS can be calculated. CVSS defines the ease of exploitation and the weight that a particular security attack and vulnerabilities could cause in a particular system. Reporting is an important part of penetration testing. In penetration testing, a comprehensive report that covers every detail of the process is critical. Re-testing is done to determine the system's security and is done after implementing the suggestions from the report.

4 Experimental Analysis

The Wi-Fi penetration testing approach is based on Kali Linux. There are four main phases in the proposed approach: preparation, information gathering, attack simulation, and reporting. The proposed approach in this research also suggested monitoring, scanning, capturing, analyzing, and password cracking techniques. This research has it that Wi-Fi penetration testing using Kali Linux has a positive effect in improving the security assessment of a given wireless communication-based computer system. In this section, manual and automated penetration testing techniques are performed for illustration as an analysis method in the research.

4.1 Conventional Penetration Testing

The conventional penetration testing techniques are more manual techniques involving tedious tasks especially code writing to run the emulated security attacks. Conventional and non-conventional penetration testing uses similar procedures and steps in conducting the security evaluation. This involves the various penetration testing stages as outlined;

4.1.1 Pre-Engagement (Planning)

This phase of penetration testing is often overlooked by most testers, yet it is just as critical as the other phases of penetration testing. The point here is to get an overview of what test the tester wants to perform. It is not detailed, but it does provide insight into the target system that will be attacked.

4.1.2 Reconnaissance

The reconnaissance phase of the penetration test is used to gather intelligent information about the system. This process is usually performed with reconnaissance tools as active or passive reconnaissance. Active reconnaissance relies entirely on active interactions with target systems. The attackers actively search for vulnerabilities in the system. On the other hand, in passive reconnaissance, the attackers use more silent methods to gather information. This process has a lower risk of exposing the attackers but is generally slow because it involves scanning the system in the background while users are still using the system. The command in [Fig. 2](#) can help list the available schemas in the current recon databases. It is a long list of scrolling to view the available schemas.

```
File Actions Edit View Help
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See '
keys add'.
[recon-ng][test] > db schema

+-----+
| domains |
+-----+
| domain | TEXT |
| notes  | TEXT |
| module | TEXT |
+-----+

+-----+
| companies |
+-----+
| company | TEXT |
| description | TEXT |
| notes   | TEXT |
| module  | TEXT |
+-----+
```

Figure 2: The current recon databases

The command in [Fig. 3](#) searches through the installed modules for the supplied module name “hack.”

```
[recon-ng][test] > db insert domains
domain (TEXT): recon-test
notes (TEXT): domain for the test project
[*] 1 rows affected.
[recon-ng][test] > modules search hack
[*] Searching installed modules for 'hack' ...

Recon
-----
recon/domains-hosts/hackertarget

[recon-ng][test] > █
```

Figure 3: Search modules

The command shown in Fig. 4 illustrates the execution command to identify any entry point into the system. The test is an imaginary domain; thus, the parameter did serve any substantial information. At this stage, ports, IP addresses, and even the physical locations are retrieved shown in Fig. 5.

```

File  Actions  Edit  View  Help

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with
  the results.

Options:
  Name      Current Value  Required  Description
  -----
SOURCE     default        yes       source of input (see 'info' for details)

Source Options:
  default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>    string representing a single input
  <path>      path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

[recon-ng][test][hackertarget] > run

-----
RECON-TEST
-----
[!] Error check your search parameter.
[recon-ng][test][hackertarget] > 

```

Figure 4: Identify any entry point into the system

```

*] -----
*] Country: None
*] Host: cnamc.bmw.com
*] Ip_Address: 122.200.123.179
*] Latitude: None
*] Longitude: None
*] Notes: None
*] Region: None
*] -----
*] Country: None
*] Host: snc.bmw.com
*] Ip_Address: 160.46.240.205
*] Latitude: None
*] Longitude: None
*] Notes: None
*] Region: None
*]

```

Figure 5: Retrieve ports, IP address, and physical locations

4.1.3 Threat Modeling

Scanning/detection involves identifying security vulnerabilities in the system. This involves a detailed investigation of the identified vulnerabilities and careful elaboration of the possible vulnerabilities that could be executed against the system. During this Metasploit find 2006 exploits, 562 payloads, and 7 evasions, as shown in Fig. 6. Threat alerts are shown in Fig. 7.



```

kali@kali: ~
File Actions Edit View Help

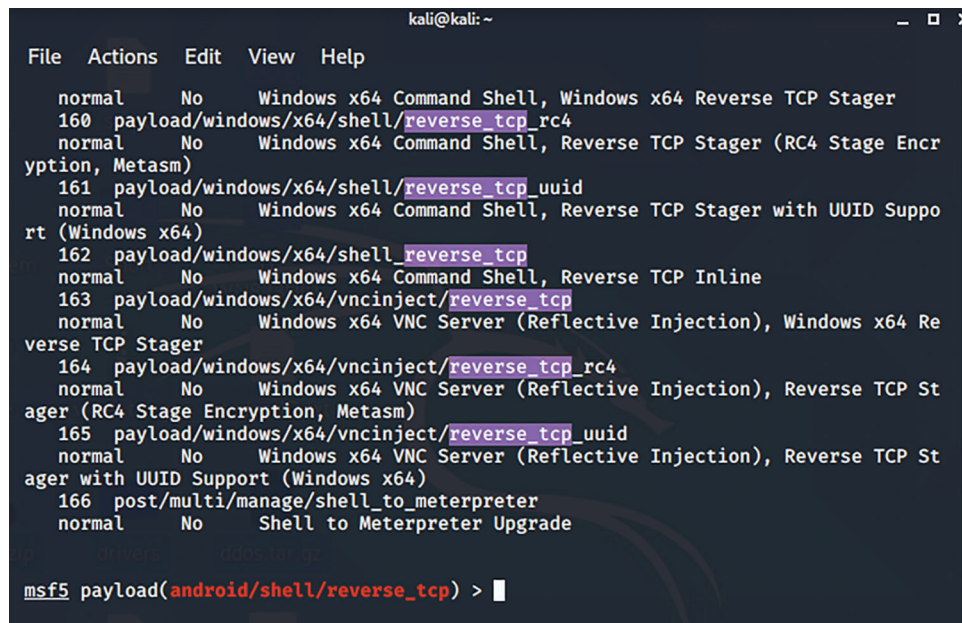
=[ metasploit v5.0.87-dev ]
+ -- --=[ 2006 exploits - 1096 auxiliary - 343 post ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

msf5 >

```

Figure 6: Msfconsole start



```

kali@kali: ~
File Actions Edit View Help

normal No Windows x64 Command Shell, Windows x64 Reverse TCP Stager
160 payload/windows/x64/shell/reverse_tcp_rc4
normal No Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encr
yption, Metasm)
161 payload/windows/x64/shell/reverse_tcp_uuid
normal No Windows x64 Command Shell, Reverse TCP Stager with UUID Suppo
rt (Windows x64)
162 payload/windows/x64/shell/reverse_tcp
normal No Windows x64 Command Shell, Reverse TCP Inline
163 payload/windows/x64/vncinject/reverse_tcp
normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Re
verse TCP Stager
164 payload/windows/x64/vncinject/reverse_tcp_rc4
normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP St
ager (RC4 Stage Encryption, Metasm)
165 payload/windows/x64/vncinject/reverse_tcp_uuid
normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP St
ager with UUID Support (Windows x64)
166 post/multi/manage/shell_to_meterpreter
normal No Shell to Meterpreter Upgrade

msf5 payload(android/shell/reverse_tcp) >

```

Figure 7: Threat alerts

4.1.4 Exploitation

The exploitation phase of penetration testing is related to threat modeling, with both presented in the same step. It is the actual implementation of the emulated security attack in the system. It is the actual implementation of the emulated security attack in the system. How to set the threat on the target IP is shown above in Fig. 7.

The above Fig. 8 indicates exploiting the weak security system in the IP address served using msfvenom, as shown in Fig. 9.

```
File Actions Edit View Help
162 payload/windows/x64/shell/reverse_tcp
normal No Windows x64 Command Shell, Reverse TCP Inline
163 payload/windows/x64/vncinject/reverse_tcp
normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
164 payload/windows/x64/vncinject/reverse_tcp_rc4
normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
165 payload/windows/x64/vncinject/reverse_tcp_uuid
normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
166 post/multi/manage/shell_to_meterpreter
normal No Shell to Meterpreter Upgrade

msf5 payload(android/shell/reverse_tcp) > msfconsole -p android/meterpreter/reverse_tcp LHOST=192.168.1.1
[-] msfconsole cannot be run inside msfconsole
msf5 payload(android/shell/reverse_tcp) > msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.1
[*] exec: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.1
```

Figure 8: Set the threat on the target IP

```
File Actions Edit View Help
^P\^R^I^P^M^E^T^A^I^N^F^/^S^I^G^N^F^I^L^E^/^.^S^F^}^5^f^*^P^2^V^T^b^j^W^k^
P[FwJ8Ft06070Z0000</>00V!LV00z00V|0?E,x00!d60~b^
.m0*P0,d0_14[00000C0>000AV00s^0>0L0~00W70M,000) f00#0P0\0R0p
.RSA3hb0c00j0h00000500]00]0000a10300000000000000qA0,0600M0312u00C
00:000g00;000
.0I00r00F0F50606Q000000F000006Q0000I00
000000LM00
02+l0m0000z0jh0000j00000"12l
!kc0sg0sH0000000A00*0s0000W00K00000v0\000hR00K00000?0y00000Z4
G000nf]5000000A00000g0Fu0C00:00<k0$0000000z21ij0I00000cZ4dRTOB00
JM0\0k0R6fF00b0000I00%00L00m0d0<0wCQ000000n0m00 0#0a0)'0Z000P$0^
0K0<L{0m0Q00000]F007'0500000p00j030!0000/0/yi00x050c
0;000000^:000\0000007[000
00000$P00000e000~007;0X{0WB00000:0W0000(k0e0\000000HD0?0TY*000:
090?00i-;T;o0hbM000611FS(0000000GM~M0
000000000000~A0r00x0qs00)0"0we4>0TW
!00000x000}00v00003k000p0A0F0E000000Q0v0k0v0z00N+09q0tv~00)00(
000x[Q0G000>eo|?bx0000000 000000-:000<0Num00\09000e0:00000230>x0}0=
$000\000|E0070 00uP0\0R000000PndroidManifest.xmlLP0\0R0000<0resources
0classes.dexPK0\0R 0META-INF/P0\0Rp]000META-INF/MANIFEST.MFP0\4
0 META-INF/SIGNFILE.SFP0\0R0p0020!META-INF/SIGNFILE.RSAPK00%
msf5 payload(android/shell/reverse_tcp) >
```

Figure 9: Msfvenom exploitation

4.1.5 Post-Exploitation

The Post-Exploitation phase of penetration testing is focused on analyzing the impact of the penetration test. This is where things like CVSS can be calculated. CVSS defines the ease of exploitation and the weight that a given security attack and vulnerabilities could cause in the given system.

4.1.6 Reporting

Reporting is an important part of penetration testing. In penetration testing, a comprehensive report that covers every detail of the process is crucial. This is where stakeholders gain insight into the appropriate solutions that can be taken against the penetration test results. A report can be either a technical report or a normal report aimed at different recipients. The report is written in a neutral form that can be understood by the non-technical stakeholders of the organization.

4.1.7 Re-Testing

Re-testing is also a part of penetration testing that is overlooked in many cases. It is, however, an essential part of penetration testing that is meant to ascertain the security of the system. After penetration testing, a re-test is done after the suggestions in the report have been implemented.

4.2 Unconventional Penetration Testing

The Unconventional means of penetration testing use more autonomous tools and techniques to run security tests. The unconventional penetration testing methods create a new dimension of automation from scanning to the re-testing phase. Automated or more unconventional penetration testing approaches have little or no human input. This makes the process much easier, unlike the conventional methods of penetration testing. The manual/conventional methods of penetration testing require resources and time to be performed. Due to these requirements, conventional penetration testing is very costly and time-consuming, so it may not be the optimal solution in the current business domain. Currently, cyberspace is experiencing massive growth in valuable information and the growing concern about security breaches.

The conventional methods of penetration testing and non-conventional penetration testing have similar outcomes and goals. The general objective of both is to detect security vulnerabilities in the system to improve the computer system's security. The difference between the two is caused by the modes of execution and the optimal aspects of the two. Of the two approaches, the non-conventional modes of penetration testing are optimal and cost-effective instead of the conventional ways of penetration testing. Technology is currently seeking automation in so many aspects of life. Computer security is one such area that is experiencing automation. Automation is a non-conventional way of penetration testing and in the future in overall computer security.

As a non-conventional penetration testing method, technology is also more effective and efficient in the data flows currently occupy cyberspace. [Tab. 1](#) shows the dynamic tools for vulnerability scan. [Fig. 10](#) shows the result by severity, and [Fig. 11](#). show the vulnerability by category, and it is caused by two main reasons. The first vulnerability is caused by human knowledge, and the second one is vulnerabilities caused by configuration. Three main weaknesses are weaknesses in databases, vulnerabilities in the network, and weaknesses in applications. The scale measurements start from 0.0 to 10.0. The 0.0 is the lowest vulnerability rate. It depicts that both human knowledge and the right configuration cannot be separated.

Table 1: Comparison of dynamic penetration testing software

Tool name	Analysis style	Language support	Cost factor	Testing style	Method	Vulnerability found	Vulnerability top language
Acuentix	Dynamic	PHP-JAVA	Commercial	Black	Runtime	41	PHP&JAVA
Nessus	Dynamic	PHP-JAVA	Commercial	Black	Runtime	44	PHP&JAVA
AppSpider	Dynamic	PHP-JAVA	Commercial	Black	Runtime	38	JAVA
BurpSuitePro	Dynamic	PHP-JAVA	Commercial	Black	Runtime	40	PHP&JAVA
NetSparker	Dynamic	PHP-JAVA	Commercial	Black	Runtime	42	JAVA

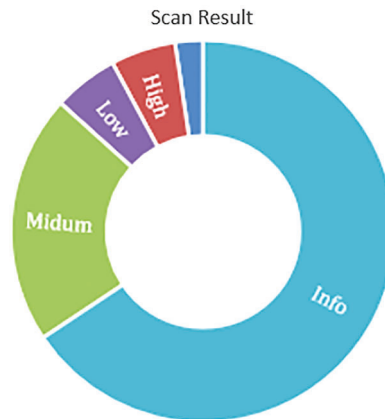


Figure 10: Scan result by severity

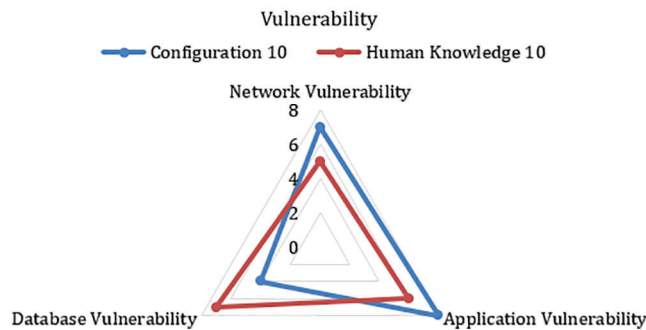


Figure 11: Vulnerability by category

Target IP- 192.168.254.133 is scanned using the Nessus tool for vulnerability scan, vulnerability is found in the range of info to critical shown in Tab. 2, The severity, CVSS, and name are shown in Tab. 3. The Common Vulnerability Scoring System (CVSS) scores are calculated using CVSS (CSV 3.0) [27].

Table 2: Vulnerability found using Nessus

Critical	High	Medium	Low
3	7	27	7

Table 3: Vulnerability scores calculated using CVSS

Severity	CVSS v 3.0	Plugin	Name
High	7.5	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability
Critical	10	58327	Samba ‘AndX’Request Heap-Based Buffer Overflow
Critical	10	61708	VNC Server ‘password’ Password
High	7.5	78515	Drupal Database Abstraction APL SQLi
High	7.5	41028	SNMP Agent Default Community Name(public)
High	7.1	2007	SSL ver.2 and 3 protocol detection
Medium	6.8	90509	Samba Badlock vulnerability
Low	5.1	71783	Network Time Protocol Daemon monlist command enabled DoS

The Base score formula discussed in [28] is used to adjust the level of vulnerability found in the range [0.0,10.0], as shown in Eq. (1).

Where B_s is the Base Score concerning vulnerability, scores range from 0 to 10, with 10 being the most severe [7]. The Base score calculated using Eq. (1) and obtained from the Exploitability metric (EM) and Impact metric (IM). EM depends on the attack vector, attack complexity, privileges and user interaction, whereas impact metric depends on confidentiality, integrity, and availability impact and produces the vulnerability of CVSS Vector.

The base score is calculated as;

Base score = Round to 1 decimal $\{[(0.6 \times \text{Impact}) + (0.4 \times \text{Exploitability}) - 1.5] \times f(\text{Impact})\}$ [28]

Where Exploitability = 20 x Access Vector x access complexity x Authentication

Impact = 10.41x (1-(1- CI) x(1-II) x(1-AI)

Where CI is confidentiality impact, II is integrity and AI is availability impact

$F(\text{Impact}) = 0$, if impact =0, otherwise it is 1.76

$$f(B_s) = \begin{cases} 0.1 < B_s < 3.9, \text{Low} \\ 4.0 < B_s < 6.9, \text{Medium} \\ 7.0 < B_s < 8.9, \text{High} \\ 8.9 < B_s < 10, \text{Critical} \end{cases} \quad (1)$$

Risk arises when threat and vulnerability intersect, and consequences and probability are accessible by the organization to reduce the risk. Consequence zero (0) means that the loss of CIA does not affect, one (1) means low, and two (2) means a high impact on trust and reputation. The likelihood is low; it means that the security controls are strong enough. High means that the security controls are very weak or ineffective [7,8]. Vulnerabilities, their impact on CIA, and computed risk given in Tab. 4. It depicts that risk levels due to V1-V6 are high, while V7-V8 are low.

Table 4: Vulnerabilities and their impact

Vulnerabilities	CVSS score	Confidentiality impact	Integrity impact	Availability impact	Access complexity	Consequence (c)	Likelihood (l)	Risk= c*l
V1	7.5	H	M	H	M	2	2	4
V2	10	H	H	H	H	2	2	4
V3	10	H	H	H	H	2	2	4
V4	7.5	H	M	H	H	2	2	4
V5	7.5	H	M	H	M	2	2	4
V6	7.1	H	M	H	M	2	2	4
V7	6.8	M	L	M	M	2	1	2
V8	5.1	M	L	M	L	1	1	1

low—L, medium—M, high—H.

While conventional means of penetration testing is the emulation of security attacks in a given system. The unconventional means of penetration testing use more autonomous tools and techniques to perform security testing. New vulnerabilities are found every day, and even the most trivial vulnerability, if properly exploited, can cause significant damage to an organization. The difference is evident in the tools used in both methods of penetration testing. Calculated vulnerabilities and risks based on CVSS scores

show that the risk due to V1-V6 is high, while V7-V8 is low. Dynamic tool scanners are commercial because large companies put a lot of effort into them. It also shows that dynamic tools are excellent in finding vulnerabilities but slower than static tools. Multiple vulnerability scanners can have multiple reports, and they also have multiple techniques to test specific types of vulnerabilities. Therefore, developers and testers should try to use multiple scanners to discover web vulnerabilities. Potential attackers are always more creative than developers, but they may have talented ideas to attack the system. Therefore, the assessment result of these vulnerabilities may not last.

5 Conclusion

In theory, traditional penetration testing approaches were effective until cyberspace changed. The changes in technology have necessitated the need for unconventional ways of penetration testing. Unconventional penetration testing tactics require less tedious writing of code and are therefore easier to manage. Unconventional penetration testing adds more to the security assessment. In addition to computer security assessment, unconventional types of penetration testing add to the list of efficiency in terms of speed and effectiveness of testing. This has led to an increase in cyberspace in terms of devices and information hosted in cyberspace. Unconventional ways of testing the security of a system are a means of time and efficiency in the security evaluation of the system. The problem with new and unconventional penetration testing methods is that they are not always a guarantee of solving security problems. This is because technology is constantly changing and is never stable at any one point in time. This means that there will always be vulnerabilities, security holes, and threats, even if unconventional methods for penetration testing emerge. The proposed Wi-Fi penetration test using Kali Linux has a positive effect in improving the security assessment of a given wireless communication-based computer system. Conventional means of penetration testing is the emulation of the security attacks in a given system. The non-conventional means of penetration testing use more autonomous tools and techniques to run security tests. The CVSS scores for scanned vulnerabilities are calculated using automated tool, the vulnerabilities and their impact on CIA and the associated calculated risk are discussed, it is shown that the risk levels due to V1-V6 are high while V7-V8 are low. Dynamic tool scanners are commercial because large companies put a lot of effort into them. It also shows that the dynamic tools are excellent in finding vulnerabilities, but it is slower than static tools. Several vulnerability scanners may have multiple reports, and they also have several techniques to test particular types of vulnerabilities. Therefore, developers and testers should attempt to use more scanners to discover web vulnerabilities. When we exploit vulnerable applications, we can imagine from our views. While possible attackers are evermore more creative than developers, they may have talented ideas to attack the system. Therefore, the evaluation result of these vulnerabilities may not be permanent. Unconventional ways of testing the security of a system are a go-to to address the issues of time and efficiency in the security evaluation of the system. It is expected that future penetration testing will also be scalable to accommodate any changes that may occur in the target system, unlike current penetration testing mechanisms that are guided by pre-built frameworks. In short, the future of penetration testing is based on automation and scalability to accommodate the rapidly growing cyberspace. Machine learning has always been at the center when it comes to automation. It is a pre-programmed approach that aims to detect security vulnerabilities. The approach is not widely used and hence is classified under the unconventional techniques of penetration testing. Markov Decision Process is one of the machine learning algorithms that can be used for this purpose. Markov Decision Process (MDP) is generally used for discrete uncertainties. Applied in penetration testing space, the state space becomes simpler for configuring the target and actions during the process. The MDP approach to penetration testing in machine learning is advantageous because it allows modeling uncertainties while maintaining the computational.

Acknowledgement: The authors sincerely acknowledge the support from Majmaah University, Saudi Arabia, for this research.

Funding Statement: The authors would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project Number No - R-2021-xx.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber- attacks," *Computers & Security*, vol. 72, no. 3, pp. 212–233, 2018.
- [2] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3, pp. 73, 2019.
- [3] M. A. Zarandi, R. A. Dara and E. Fraser, "A survey of machine learning-based solutions to protect privacy in the Internet of Things," *Computers & Security*, vol. 96, pp. 1–9. 2020. https://www.sciencedirect.com/science/article/pii/S0167404820301978?casa_token=z4q31gkG6NUAAAAA:TYRLj6ebx4Z4xL-9l9Pw2rkPWm62IVdaZloFK6CCyDVEidkvtGOolf9PdVRkeWdtonok6dgI6QKzIA.
- [4] J. P. Yaacoub, N. Hassan, O. S. Noura and A. Chehab, "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, vol. 15, no. 1, pp. 172988141875942, 2021.
- [5] G. Nguyen, S. Dlugolinsky, V. Tran and A. L. Garcia, "Deep learning for proactive network monitoring and security protection," *IEEE Access*, vol. 8, pp. 19696–19716, 2020.
- [6] P. Mikalef and M. Gupta, "Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance," *Information & Management*, vol. 58, no. 3, pp. 103434, 2021.
- [7] S. Mishra, S. K. Sharma and M. A. Alowaidi, "Analysis of security issues of cloud-based web applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1–12, 2020.
- [8] S. Mishra, M. A. Alowaidi and S. K. Sharma, "Impact of security standards and policies on the credibility of e-government," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1–12, 2021.
- [9] M. C. Ghanem and T. M. Chen, "Reinforcement learning for efficient network penetration testing," *Information-an International Interdisciplinary Journal*, vol. 11, no. 1, pp. 6, 2020.
- [10] J. N. Goel and B. M. Mehtre, "Vulnerability assessment & penetration testing as a cyber-defense technology," *Procedia Computer Science*, vol. 57, pp. 710–715, 2015.
- [11] K. Coffey, R. Smith, L. Maglaras and H. Janicke, "Vulnerability analysis of network scanning on SCADA systems," *Security and Communication Networks*, vol. 2018, no. 4, pp. 1–21, 2018.
- [12] M. Moyo and M. Looock, "Conceptualising a cloud business intelligence security evaluation framework for small and medium enterprises in small towns of the limpopo province, south africa," *Information-an International Interdisciplinary Journal*, vol. 12, no. 3, pp. 128, 2021.
- [13] G. Cascavilla, D. A. Tamburri and W. J. V. D. Heuvel, "Cybercrime threat intelligence: A systematic multi-vocal literature review," *Computers & Security*, vol. 105, no. 3, pp. 102258, 2021.
- [14] A. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar *et al.*, "Penetration testing framework for smart contract Blockchain," *Peer-to-Peer Networking and Applications*, vol. 5, no. 2, pp. 303, 2020.
- [15] N. R. Moşteanu, "Challenges for organizational structure and design as a result of digitalization and cybersecurity," *The Business & Management Review*, vol. 11, no. 1, pp. 278–286, 2020.
- [16] W. A. Al-Khater, S. Al-Maadeed, A. Ahmed, A. S. Sadiq and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020.
- [17] E. Tufan, C. Tezcan and C. Acartürk, "Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network," *IEEE Access*, vol. 9, pp. 50078–50092, 2021.

- [18] O. M. Al-Matari, I. M. Helal, S. A. Mazen and S. Elhennawy, "Integrated framework for cybersecurity auditing," *Information Security Journal: A Global Perspective*, vol. 29, pp. 1–16, 2020. https://www.tandfonline.com/doi/full/10.1080/19393555.2020.1834649?casa_token=o6r0fO_IccoAAAAA%3AKpbWqmUGxwF8yHmDe7yfKB4grKWnmlVLVHdKn5WQzF1dv5uXazPyr0EBBfKPDCzKjXAPV4QfzcKCOXPg.
- [19] A. J. V. Vaca, R. M. Gasca, J. A. C. Fombella and M. T. G. Lopez, "AMADEUS: Towards the AutoMated secUrity testing," in *Proc. of the 24th ACM Conf. on Systems and Software Product Line: Volume A-Volume A*, New York, NY, United States, pp. 1–12, 2020.
- [20] W. Steingartner, D. Galinec and A. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model," *Symmetry*, vol. 13, no. 4, pp. 597, 2021.
- [21] S. Y. Enoch, Z. Huang, C. Y. Moon, D. Lee, M. K. Ahn *et al.*, "HARMer: Cyber-attacks automation and evaluation," *IEEE Access*, vol. 8, pp. 129397–129414, 2020.
- [22] D. Upadhyay and S. Sampalli, "SCADA (supervisory control and data Acquisition) systems: Vulnerability assessment and security recommendations," *Computers & Security*, vol. 89, no. 3, pp. 101666, 2020.
- [23] I. Bastys, M. Balliu, T. Rezk and A. Sabelfeld, "Clockwork: Tracking remote timing attacks," in *2020 IEEE 33rd Computer Security Foundations Sym. (CSF)*, Boston, MA, USA, pp. 350–365, 2020.
- [24] V. Bolbot, G. Theotokatos, E. Boulougouris and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Safety Science*, vol. 131, pp. 104908, 2020.
- [25] F. Kamoun, F. Iqbal, M. A. Esseghir and T. Baker, "AI and machine learning: A mixed blessing for cybersecurity," in *2020 Int. Sym. on Networks, Computers and Communications (ISNCC)*, IEEE, Montreal, QC, Canada, pp. 1–7, 2020.
- [26] K. Scarfone, M. Souppaya, A. Cody and A. Orebaugh, "NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2008. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>.
- [27] Common Vulnerability Scoring System (CVSS), "NIST Computer Security Division. Gaithersburg, MD, USA: Information Technology Laboratory. 2019. [Online]. Available: <https://nvd.nist.gov/vuln-metrics/cvss>.
- [28] P. Mell, K. Scarfone and S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0," in *Published by FIRST-forum of incident response and security teams*. vol. 1, pp. 1–23, 2007.