ISSN: 0974-5823 Vol. 7 No. 1 January, 2022

International Journal of Mechanical Engineering

Software Security Testing Types and their Evaluation against the Testing Metrics

Shantanu Mukherjee
Brainware University, Barasat, India

Sandip Roy
Brainware University, Barasat, India

Pinaki Pratim Acharjya
Haldia Institute of Technology, Haldia, India

Abstract.

Information security is the buzzword at the moment. With so much of data and information floating around, everyone is concerned about its securi- ty far more than ever before. However, the question that haunts everyone is, "Is the data really secured"? It is imperative that we define a security measurement mechanism to identify how much security is optimum for a particular scenario. Security measurement has always been at the bottom of the priority list and so it is far from being developed. A success factor should not be just to prevent unauthorized data access and maintaining the confidentiality and sanctity of the data but to gauge the impor- tant parameters and their contribution to maintain the security of the data. In- formation security means preventing unauthorized access to data for any nefa- rious purpose, including but not limited to, their usage, alteration or modifica- tion and disclosure.

Keywords: Information Security, Security Assessment, Vulnerability Scanning, Security Testing, Performance Metrics

1 Introduction

Information security has to be imbibed and developed as an inherent activity instead of an additional technical task. The entire security facet is dependent on the founda- tion of risk assessment and its impact, which if not given due weightage, may cause a potential source of vulnerability and an attack point for all hackers. The process of information security measurement starts with identifying the entities and their role in the security infrastructure. These entities could be a host, an API, the network, the user or anything or anyone that accesses the data [1]. The focus should not be on whether there is a proper security infrastructure in place or not but it should be more on how closely it is aligned to the business strategy of the organization, which directly impacts the overall business performance [2]. The approach route to measuring in- formation security is highlighted in the following figure:

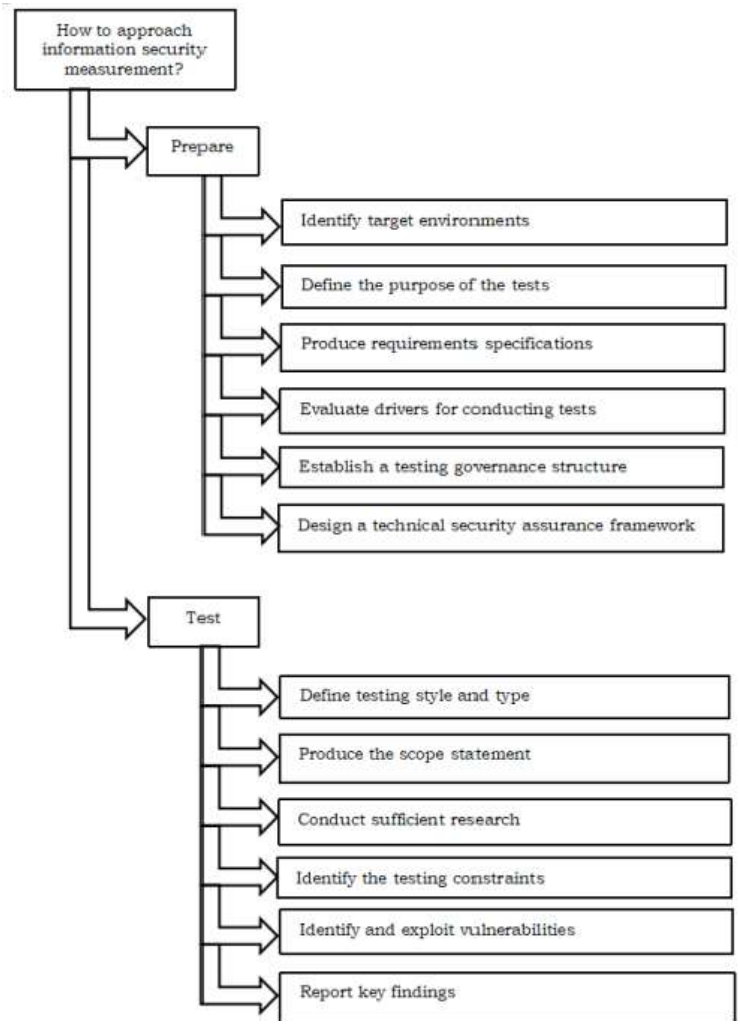

Fig. 1. Steps in Information Security Measurement

1.1 Preparation

The preparation phase starts with identifying what to test. The objective of the prepa- ration phase should be to uncover the information required for a comprehensive test- ing in the next stage. This can involve identifying the entities to be tested, the right testing technique and the attacking mechanism to be employed, the threats and their possible impact, the risk mitigation strategies in place and their effectiveness etc. [3][4]. This step requires an in-depth study of the application and avoid any cursory review since it may be quite vague and allure you to overlook major security pitfalls in the application. Thus, the project manager needs to visualize the complete applica- tion from an abstract level of operational and management standpoint and analyze the consequences of its failure rather than just testing the technical implementation of the application [5].

1.2 Testing

The security landscape is flooded with numerous testing mechanism and this, at times, can be overwhelming to the security tester. The main objective of security test- ing is to discover the vulnerabilities and devise appropriate remedial actions to pre- vent the hacker from exploiting them [6][7][8]. The testing procedure includes scan- ning and penetration techniques to unearth the security loopholes. Testing could be
external or internal. External testing is like viewing the system from internet and ry-
ing to break the security posture in order to identify the vulnerabilities that may be exploited by an attacker [9]. For internal security testing the attack is more from with- in the security perimeter whereby the assumption is, that the attacker is able to pene- trate the security defenses and carrying out the attacks [10].

1.3 Follow-up

Follow-up is the most important phase once the testing is completed. It encompasses summarizing the findings and implementing appropriate remediation strategies. It should also mention the best practices to be adhered to, to prevent possible abuse of the

system [11]. The following figure illustrates the major steps in the follow-up phase.

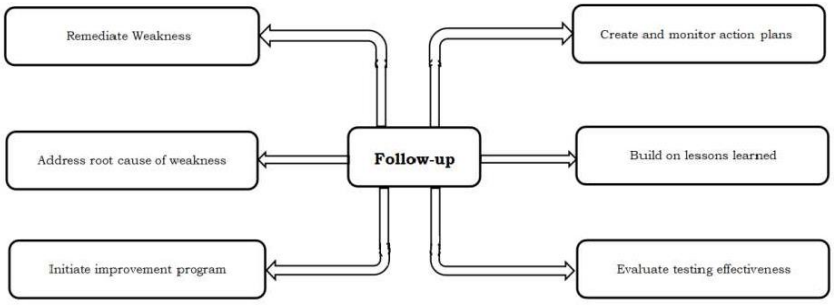

Fig. 2. Various Action Items in the Follow-up phase

2 Target Vulnerability Detection Techniques

As mentioned earlier that there are numerous types of security testing, so this section highlights the factors on which an appropriate testing technique may be chosen. The testing techniques could be manual or automated but they rely on human intelligence, knowledge, and experience for result interpretation [12][13].

2.1 Network Scanning

Network scanning starts with discovering the devices that have a network address or are accessible to another device in the address space. The scanners not only identify the active hosts and open ports but also perform operating system fingerprinting, that is, identifying the target operating system [14]. This when amalgamated with addi- tional information of the application running on a particular port may provide a start- ing point for the attacker intending to bring down the application. Although network scanning leads to identifying the active hosts, applications, services and operating system but the actual discovery of the vulnerabilities is possible only by an expert who can infer from the scan results [15][16]. The following figure illustrates the pros and cons of network scanning.

2.2 Vulnerability Scanning

Vulnerability scanners address the limitations faced by the port scanners. They not only identify the hosts and the open ports but also highlight the potential vulnerabili- ties with possible mitigation strategies. These scanners help in indicating the organi- zations' risk exposure [17]. Vulnerability scanners first performs operating system fingerprinting to identify the operating system and then employs a large database to find matching known exposures and their mitigation strategies [18]. Although vulne- rability scanners are far more efficient than the network scanners but the downside is that they generate a relatively more traffic on the network and have high rates of false positives.

2.3 Log Reviews

Now a days, any application to be accessed over the network is built to log huge amounts of data. These logs may include data such as the logs from the servers, the intrusion detection systems, the firewalls etc. Auditing these logs from time to time may provide clue to suspicious activities. For instance, the IDS logs can reveal unau- thorized access penetrating through the firewalls [19][20]. A very commonly used IDS sensor is Snort. Snort is an open-source IDS sensor, that can perform real-time traffic analysis and packet logging on IP networks. Log reviews on the main servers and the firewalls should be done very meticulously on a regular basis to identify the bottlenecks before they can be discovered and exploited by the attackers [21].

2.4 File Integrity Checkers

These are the tools generally employed by the system admins to detect unauthorized changes to guarded files. They calculate and store a checksum for the sensitive files and maintain a database for the file checksums [22][23]. These stored values of checksums are checked against the recalculated values on a regular basis to identify file changes. In case, the integrity checker detects an unauthorized file modification then it should necessitate a thorough investigation as per the organizations' security policies [24].

2.5 Penetration Testing

This procedure is used by the security testers to gain access to the system by adopting the tactics commonly used by the attackers. Although, penetration testing is quite labor intensive and requires high level of skills but they are unparalleled in their ca- pabilities of detecting vulnerabilities and securing the application against attackers [25][26]. Penetration testing consists of four phases as shown in the figure below:

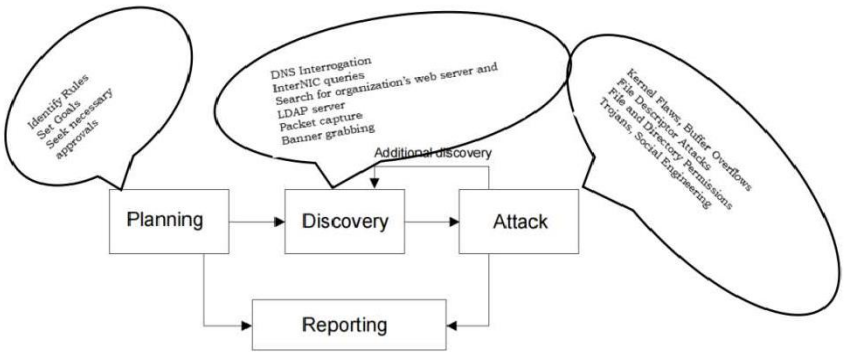

Fig. 3. Four Phases of Penetration Testing

3 Comparison Summary of the Network Testing Techniques

Table 1. The Pros and Cons of the Testing Techniques

Testing Type	Pros	Cons
Network Scanning	Fast Efficiently scans hosts, depending on number of hosts in network Many open-source tools available Automated	Does not directly identify known vulnerabilities Generally used as a prelude to penetration testing not as final test Requires significant expertise to interpret results
Vulnerability Scanning	Low cost Can be fairly fast Highly automated Identifies known vulnerabilities Often provides advice on mitigat-	Has high false positive rate Generates large amount of traffic aimed at a specific host (which can cause the host to crash or lead to a

	ing discovered vulnerabilities Easy to run on a regular basis	temporary denial of service) Identifies only surface vulnerabilities Requires great expertise
Penetration Testing	Tests network using the metho- dologies and tools that attackers employ Goes beyond surface vulnerabili- ties and demonstrates how these vulnerabilities can be exploited Can provide the realism and evi- dence needed to address security issues Social engineering allows for testing of procedures and the human element	Very labor intensive Slow, target hosts may take hours/days to "crack" Due to time required not all hosts on medium or large sized networks will be tested individually Certain tools and techniques may be banned or controlled by agency regu- lations (e.g., network sniffers, pass- word crackers, etc.) Expensive
Log Reviews	Only data source that provides historical information	Cumbersome to manually review Automated tools not perfect can filter out Important information
File Integrity Checkers	Reliable method of determining whether a host has been compro- mised Highly automated Low cost	Does not detect any compromise prior to installation Checksums need to be updated when system is updated Checksums need to be protected (e.g., read only CD-Rom) because they provide no protection if they can be modified by an attacker

Security tests should include carrying out sufficient research to imitate the research activities that a potential attacker could undertake to find out as much about the target environment and how it works as possible. Research undertaken should include gathering, collating and analyzing all relevant information about the target environment [27]. Typical techniques are described in the figure below.

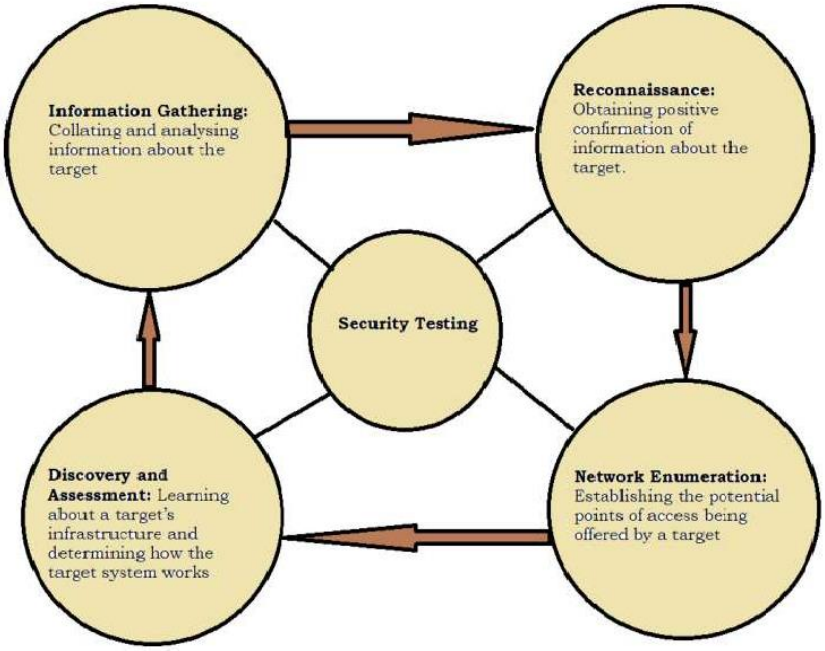

Fig. 4. Security Testing Techniques

4 Measurement Metrics

This section lists a set of security and performance metrics, mainly focusing on net- work vulnerability assessment, attack risk evaluation, and mission impact analysis. Each of the metric defined in table below attempts to answer a specific question re- lated to the computer/network security, system performance, or mission assurance [28][29]. For instance, the Vulnerable Host Percentage (VHP) metric tries to answer how many hosts could be compromised in the worst case. The Average Length of Attack Paths (ALAP) metric attempts to answer the typical effort required for an at- tacker to violate a security policy. Obviously, each metric has shortcomings if only used by itself for the security analysis. For example, the Shortest Attack Path (SAP) metric ignores the number of ways an attacker may violate a security policy; the ALAP metric fails to adequately account for the number of ways an attacker may violate a security policy; while the Number of Attack Paths (NAP) metric ignores the effort associated with violating a security policy [30][31][32]. Therefore, multiple security metrics must be used together to provide users with a comprehensive v ew and understanding of cyber situational awareness and mission assurance.

Table 2. Common Security and Performance Metrics

Metric	Acronym	Description	Testing Type that can detect
Asset Capacity	AC	The (remained) capacity of a cyber asset (after being attacked or compromised)	Network Scanning Vulnerability Scanning Penetration Testing Log Review File Integrity Checkers
Average Length of Attack Paths	ALAP	The average effort to penetrate a network, or compromise a system/service; evaluated by attack graphs	Network Scanning Vulnerability Scanning Penetration Testing
Compromised Host Percentage	CHP	The percentage of compromised hosts in a network at time t	Network Scanning Vulnerability Scanning Penetration Testing File Integrity Checkers
Exploit Probability	EP	How easy (or hard) to exploit a vulnerability? Could be measured by CVSS	

exploitability sub-score			Vulnerability Scanning Penetration Testing Log Review
Impact Factor	IF	The impact level of a vulnerability after being exploited, could be measured by CVSS impact sub-score	Vulnerability Scanning Penetration Testing Log Review
Number of Attack Paths	NAP	The number of potential attack paths in a network, could be evaluated based on attack graphs	Penetration Testing Log Review
Network Preparedness	NP	Is a network ready to carry out a mission? E.g., all required ser- vices are supported by available cyber assets	Penetration Testing
Network Resilience	NR	The percentage of compromised systems/services that can be replaced/recovered by back- up/alternative systems/services	Penetration Testing
Operational Capacity	OC	The (remained) operational capacity of a system/service (after being affected by a direct attack or indirect impact)	Penetration Testing Log Reviews
Resource Redundancy	RR	Are there any redundant (back- up) resources assigned or allo- cated for a critical task/operation?	Vulnerability Scanning Penetration Testing
Service Availability	SA	The availability of a required	Vulnerability Scanning

		service to support a particular mission, task, or operation	Penetration Testing Log Review Penetration Testing Log Reviews
Shortest Attack Path	SAP	The minimal effort to penetrate a network, or compromise a system or service, evaluated by attack graphs	Vulnerability Scanning Penetration Testing Log Review
Severity Score	SS	The severity/risk of a vulnerability if it was successfully exploited, could be measured based on CVSS score	
Vulnerable Host Percentage	VHP	The percentage of vulnerable hosts in a network	Network Scanning Vulnerability Scanning Penetration Testing Log Review

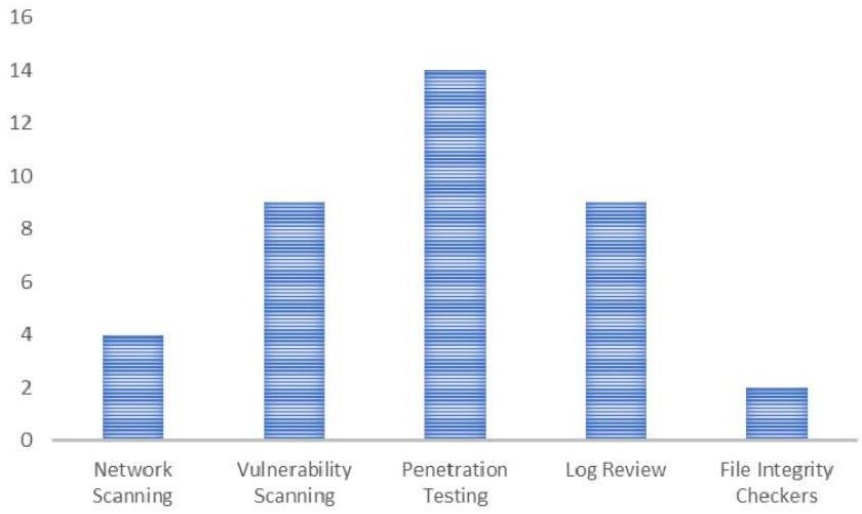

Fig. 5. Utility of various testing types against the testing metrics

5 Conclusion

There are typically aspects of the business that cannot be tested due to the operational limitations. However, attackers often do whatever it takes to penetrate an organization or system. If they are not able to penetrate a particular system, they may simply try another route. So, it is a good idea to simulate live tests as closely as possible. Tes ers have limited time for testing, attackers on the other hand have unlimited time to mount a concerted attack against a system if they have the motivation, capability and resources to do so. Therefore, it becomes necessary to invest more time in testing critical systems, provide testers with as much background information as possible, thereby reducing the reconnaissance time and increasing testing time. The crux of the matter is penetration testing should be conducted on a regular basis, rather than as a one-off exercise.

References

1. Thomas, T.W., Tabassum, M., Chu, B. and Lipford, H. "Security during application devel- opment: An application security expert perspective," in Proc. The 2018 CHI Conf. on Hu- man Factors in Computing Systems, New York, NY, USA, 2018
2. Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., and Airola, A., "Ai in cy- bersecurity education-a systematic literature review of studies on cybersecurity moocs," in 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)
3. Bozic, J., and Wotawa, F. (2018). Planning-based security testing of web applications. In Proceedings of the 13th international workshop on automation of software test (AST'18)
4. Raunak, M., Kuhn, D., Kacker, R. (2017). Combinatorial testing of full text search in web applications. In 2017 IEEE international conference on software quality, reliability and se- curity companion (QRS-c)
5. Simos, D.E., Bozic, J., Garn, B., Leithner, M., Duan, F., Kleine, K., Lei, Y., Wotawa, F. (2018). Testing TLS using planning-based combinatorial methods and execution frame- work. In Software quality journal (2018)
6. Camacho, C.R., Marczak, S., Cruzes, D.S.: Agile team members perceptions on non- functional testing: influencing factors from an empirical study. In: ARES 2016, pp. 582– 589 (2016)
7. Shmaryahu, D., Shani, G., Hoffmann, J., Steinmetz, M. (2018). Simulated penetration test- ing as contingent planning. In Proceedings of the twenty-eighth international conference on automated planning and scheduling (ICAPS 2018)
8. Parkinson B, Millard DE, O'Hara K, Giordano R. The digitally extended self: a lexicologi- cal analysis of personal data. J Info Sci. 2018; 44(4): 552- 565
9. Backes, M., Hoffmann, J., Kunnemann, R., Speicher, P., Steinmetz, M. (2017). Simulated penetration testing and mitigation analysis. arXiv:1705.05088 (2017)
10. Tyagi S and Kumar K. 2018, 2018 Fifth International Conference on Parallel, and Grid Computing (PDGC)
11. Rezvani, M., Ignjatovic, A. and Bertino, E., 2018. ACM Transactions on Internet Technol- ogy 18 55:-1-1
12. Harrell, Christopher R., et al. "Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions." 2018 IEEE International Con- ference on Intelligence and Security Informatics (ISI). IEEE, 2018
13. Aarya, P. S., et al. "Web Scanning: Existing Techniques and Future." 2018 Second Inter- national Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2018
14. Wang, Y., Bai, Y., Li, L., Chen, X. and Chen, A., 2020, June. Design of Network Vulne- rability Scanning System Based on NVTs. In 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC) (pp. 1774-1777). IEEE

15. Suroto, S., 2018. WLAN Security: Threats and Countermeasures. JOIV: International Journal on Informatics Visualization, 2(4), pp.232-238
16. Kumar, G., Saha, R., Singh, M. and Rai, M.K., 2018. Optimized packet filtering honeypot with snooping agents in intrusion detection system for WLAN. International Journal of In- formation Security and Privacy (IJISP), 12(1), pp.53-62
17. Rahalkar, S., 2019. OpenVAS. In Quick Start Guide to Penetration Testing (pp. 47-71). Apress, Berkeley, CA
18. Singh, H. and Singh, J., 2017. Penetration Testing in Wireless Networks. International Journal of Advanced Research in Computer Science, 8(5
19. Bridges, R. A., Glass-Vanderlan, T. R., Iannacone, M. D., Vincent, M. S., and Chen, Q., "A survey of intrusion detection systems leveraging host data," ACM Computing Surveys, vol. 52, no. 6, pp. 1–35, 2020.
20. Tamburri, D. A., "Design principles for the general data protection regulation (GDPR): a formal concept analysis and its evaluation," Information Systems, vol. 91, Article ID 101469, 2020
21. Seo, S., and Kim, D., "Study on inside threats based on analytic hierarchy process," Sym- metry, vol. 12, no. 8, p. 1255, 2020
22. Nagendran K, Adithyan A, Chethana R, Camillus P, Bala Sri Varshini K B ,Web Applica- tion Penetration Testing ISSN: 2278-3075, Volume-8 Issue-10
23. Nirmal, K., Janet, B., and Kumar, R., "Web Application Vulnerabilities – The Hacker's Treasure," 2018 International Conference On Inventive Research In Computing Applica- tions (Icirca), Coimbatore, India, 2018
24. Votipka, D., Stevens, R., Redmiles, E., Hu, J., and Mazurek, M., "Hackers vs. testers: A comparison of software vulnerability discovery processes," in 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018, pp. 374–391
25. Furnell, S., and Bishop, M., Addressing cyber security skills: the spectrum, not the silo,
26. Computer Fraud & Security, Volume 2020, Issue 2, 2020, Pages 6-11, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(20)30017-8. (https://www.sciencedirect.com/science/article/pii/S1361372320300178)
27. Ebert, C., Ray, R. Penetration Testing for Automotive Cybersecurity. ATZ Electron Worldw 16, 16–22 (2021). https://doi.org/10.1007/s38314-021-0629-4
28. Applebaum, A., Miller, D., Strom, B., Foster, H., Thomas, C.: Analysis of automated ad- versary emulation techniques. In: Proceedings of the Summer Simulation Multi- Conference, pp. 1–12 (2017)
29. Ek, D., Petersson, J.: Abstraction of MITRE ATT&CK. Bachelor's thesis, KTH Royal In- stitute of Technology, Stockholm, Sweden (2020)
30. Johnson, P., Lagerström, R., Ekstedt, M.: A meta language for threat modeling and attack simulations. In: Proceedings of the 13th International Conference on Availability, Reliabil- ity and Security, p. 38. ACM (2018)
31. Katsikeas, S., Johnson, P., Hacks, S., Lagerström, R.: Probabilistic modeling and simula- tion of vehicular cyber attacks: An application of the meta attack language. In: Proceed- ings of the 5th International Conference on Information Systems Security and Privacy (ICISSP) (2019)
32. Meszaros, J., Buchalcevova, A.: Introducing ossf: a framework for online service cyberse- curity risk management. Comput. Security 65, 300–313 (2017)
33. Matrawy, K. K. "Modeling and Performance Evaluation of an Indirect Solar Desalination System." International Journal of Mechanical Engineering (IJME) 6.4 (2017): 1-14.
34. Rishipal, Swarna Torgal, M. P. Kamath, and A. S. Joshi. "Simple Technique for Fabrica- tion of Toroidal Surface with a Bender and Cylindrical Polishing Machine." International Journal of Mechanical Engineering (IJME) 6.4 (2017): 15-26.
35. Luhulima, Richard B. "An Investigation Into The Resistance Of Displacement Trimaran: A Comparative Analysis Between Experimental And Cfd Approaches." International Journal of Mechanical Engineering (IJME) 6.5 (2017) 9-18
36. Kumar, Dipu, and Mohammad UL Hassan. "Experimentation and Performance Evaluation of Heat Recovery from Domestic Refrigerator." International Journal of Mechanical Engi- neering (IJME) 7.3 2018 41-50
37. Kumar, Arun, and S. K. Verma. "Performance Analysis of Staggered Wire Mesh Matrix Regenerative Heat Exchanger." International Journal of Mechanical Engineering (IJME) 7.5 (2018): 11-18.
38. Kamanzi, Janvier. "Development Of A Remotely Controlled Vehicle." International Jour- nal of Mechanical Engineering (IJME) 9.1 (2020) 7-20