International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 1, February 2023, pp. 561~570
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i1.pp561-570

Response time optimization for vulnerability management system by combining the benchmarking and scenario planning models

Arif Basuki, Andi Adriansyah
Department of Electrical Engineering, Universitas Mercu Buana, Jakarta, Indonesia

Article Info

Article history:

Received Oct 27, 2021
Revised Sep 1, 2022
Accepted Sep 22, 2022

Keywords:

Network
Port scanning
Vulnerability

ABSTRACT

The growth of information and communication technology has made the internet network have many users. On the other side, this increases cybercrime and its risks. One of the main attack targets is network weakness. Therefore, cyber security is required, which first does a network scan to stop the attack. Points of vulnerability on the network can be discovered using scanning techniques. Furthermore, mitigation or recovery measures can be implemented. However, it needs a short response time and high accuracy while scanning to reduce the level of damage caused by cyber-attacks. In this paper, the proposed method improves the performance of a vulnerability management system based on network and port scanning by combining the benchmarking and scenario planning models. On a network scanning to discover open ports on a subnet, Masscan can achieve response times of less than 2 seconds, and on scenario planning for detection on a single host by Nmap can reach less than 4 seconds. It was combining both models obtained an adequate optimization response time. The total response time is less than 6 seconds.

Corresponding Author:

Andi Adriansyah
Department of Electrical Engineering, Universitas Mercu Buana
St. Meruya Selatan, Kembangan, Jakarta 11650, Indonesia
Email: andi@mercubuana.ac.id

1. INTRODUCTION

The more connected people are to one another, the easier it is to connect to the internet. As a result, the growth of cybercrime and its associated risks have increased. Cybersecurity breaches have resulted in several incidents such as exposure of personal information, theft of credit cards, loss of medical records, corporate hacking, and attacks on government [1]–[4]. The internet is a computer network system that connects all devices worldwide. Almost all human and machine activities can be served via the internet, and many devices, such as smartphones, computers, sensors, and so on, are connected to this network. As a result, internet users have increased dramatically [5], [6]. In addition, cybersecurity is an action to stop or restrict other parties from entering the network. Therefore, cyber security is closely related to the risk management process. Protecting assets in the form of a network by managing vulnerabilities can become threats that pose risks. Furthermore, security measures are taken to effectively overcome the hazards to control the system [1]. Therefore, vulnerability is a vital aspect of risk management. The action to discover network vulnerability points is to perform a scan. This scanning technique looks for vulnerabilities in terminals massively by performing a comprehensive port scan of problem areas [7], [8]. While a network is scanning, port discovery accuracy and scan response times are variables of the performance of this technique. Therefore, cybersecurity is urgent to protect immediately by cybersecurity, especially when an attack has occurred. However, before

taking security anticipations by blocking or limiting networks, it is necessary to know the location of the weaknesses. One of the best ways to discover those weaknesses is through vulnerability scanning, which determines the position of the vulnerability on the network [9]–[13].

Some studies related to network scanning have been conducted regarding the publications. This section describes some of these writings. In [14], [15], authors proposed an approach that allows tracking port scanning behavior patterns among multiple probed ports and identifies the intrinsic properties of the observed ports. The method is fully automated based on graph modelling and data mining techniques, including text mining. Niedermaier *et al.* [16] introduced network scanning and mapping as a building block to scan directly from the industrial internet of things (IIoT) edge node devices. The module scans the network in a pseudo-random periodic manner to discover devices and detect changes in the network structure. Finally, the research of [17]–[19] addresses the problem of recognizing what network scanner generated the probing packets collected by the monitored network. The methodology developed and proposed leverages hidden Markov models to model two network scanners: Zmap and Shodan. The obtained models have been then leveraged to recognize the network scanner that originated freshly collected probes.

This study aims to propose a method to improve the performance of a vulnerability management system by implementing network and port scanning based on a combination of benchmarking and scenario planning models. This paper describes knowing where these vulnerability points are and making adequate security protections. The research begins with planning the experimental flow, software and tools, network design, and experimental scenarios. Then the experiment was implemented, starting with testing three network scanning techniques using the benchmarking model. The initial test results were evaluated and combined with a scenario planning model [20] by performing a case simulation scan for vulnerability detection. The test would be performed by scanning the network with a target machine globally but limited to vulnerability scanning functionality on the internet network subnet. Therefore, the data used in this study is open network data on the Internet network. The experiment's final results were analyzed to conclude in the closing section.

2. MATERIALS AND METHOD

2.1. System design

This research contributes to optimizing the performance of a vulnerability management system based on network and port scanning by combining the benchmarking and scenario planning models. The benchmarking model was chosen to evaluate the experiment based on the network's performance comparisons of some open port scanning techniques. The scenario planning model was chosen to assess the investigation by scanning an internet protocol (IP) address with an open port to detect vulnerabilities on that port or IP address. Combining the benchmarking with scenario planning models can make a more effective solution to identify vulnerabilities on a network faster. The research flow chart is shown in Figure 1.

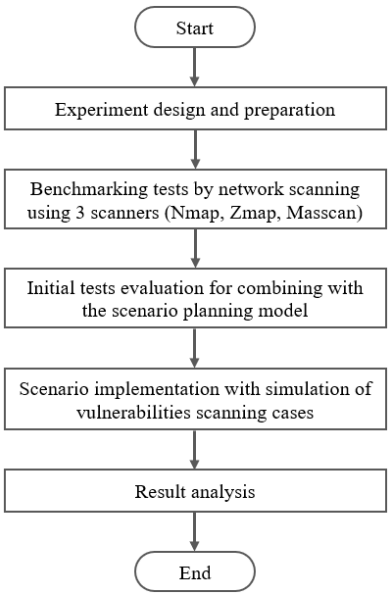


Figure 1. Research flow chart

2.2. Software and tools preparation

This research implements Linux operating system, virtualization software, and three network scanners Nmap, Zmap, and Masscan [21], [22]. It also uses a Lenovo laptop computer, ThinkPad 13, with x64 processor specifications, Intel Core i5-7200U, 2.5 GHz, 64-bit Operating System, and 10 Mbps internet connection. Further information about the network scanners and other software that were used in this research is listed in Table 1.

Table 1. Software and tools for research

No.	Softwares	Version	Remarks
1.	Nmap	7.80	Network scanner
2.	Zmap	2.1.1	Network scanner
3.	Masscan	1.0.5	Network scanner
4.	Kali Linux	5.6.0	Operating system
5	Virtual Box	6.1.10	Virtualization
6.	Windows	10	Operating system

2.3. Network design

The first implementation is some tests with a benchmarking model in this study. The tests of three network scanning techniques have been performed to compare their process and performance on a port scan to find active hosts or IP addresses with open ports. The indicators used as benchmarks are accuracy and response time. The accuracy variable (in percentage) is the level of ability of the scanning technique to perform a port search, determined from the number of ports found against the number of target ports. The response time (in seconds) is the time of the scanning to port search duration. The comparison aims to find gaps between the performance indicators among the three scanning techniques to establish new standards and improve processes.

The scan target scope resides on a network subnet. The comparison of the three scanning techniques is based on the network's port search performance of all hosts or IP addresses with Nmap, Zmap, and Masscan applications. The scanning tests are performed on an internet network using TCP/IP communication and internet network protocol version 4. (IPv4). This study makes use of network-wide open data. The scanning software is installed on a computer with the IP address 192.168.1.10.

The scan target hosts were at IP addresses from 111.221.46.0 to 111.221.46.255, 256 ports in the benchmarking tests, as shown in Figure 2. This is because the target port for network scanning is port 80 on each IP address, which is commonly used for web traffic with HTTP services [23]. The benchmarking tests implement three network scanners, Nmap, Zmap, and Masscan. They work at the same network, bandwidth, target IP address, port position, the same operating system, and the same variables for command lines. Nmap: $ nmap -p 80 xxx.xxx.xxx.0/24, Zmap: $ zmap -p 80 results.csv xxx.xxx.xxx.0/24, Masscan: $ masscan -p 80 xxx.xxx.xxx.0/24. The network scanners were conducted in a port scan, the usual initial vulnerability scanning procedure. Its function is to find an open, active port. Ports like these are points of vulnerability that third parties could exploit.

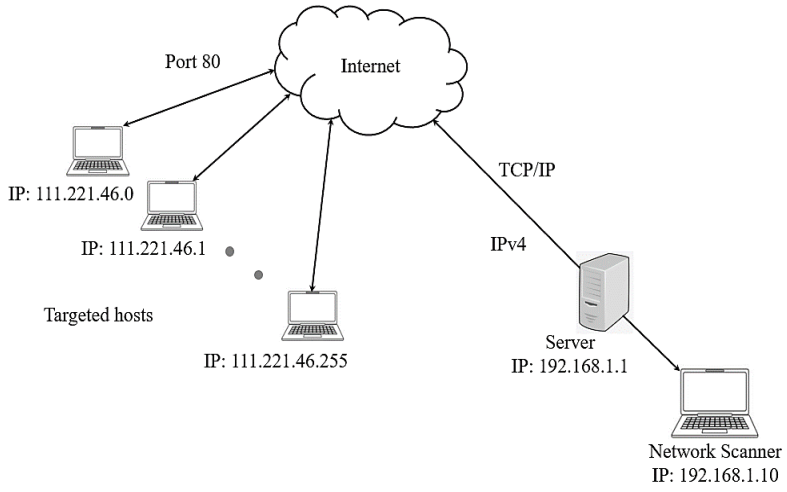


Figure 2. Testbed for benchmarking model

The indicators against which the test is measured are accuracy and response time. Accuracy (in percentage) is the level of ability of the scanning technique to perform a port search, known from the number of ports found against the number of target ports. In addition, another indicator is the response time (in seconds) or the duration of the instructed port search. Each scan test was performed ten times. The test results are evaluated and compared with each other based on these indicators.

Next, the scenario planning model experiment is performed by conducting case simulations. The target of the scan is a host server that is suspected of having a WannaCry malware attack [24]. The scanning target is a host with the IP address of 111.221.46.139, one of the target IP addresses in the network scan in the benchmarking tests, as depicted in Figure 3.

In this case simulation, the performance of port scanning is evaluated for vulnerability detection on specific open ports due to network scanning in the initial experiment. In the scenario planning model, two condition flows are simulated. Each condition has a different scanning process, as shown in Figure 4. Condition 1-has no information about the attacker, condition 2-already know the type of malware. In this case, the malware is WannaCry [24]. This case simulation aims to find the best technique to anticipate a cyber-attack. The indicator used as a reference is the response time. The target ports are in the host with the IP address 111.221.46.139, as depicted in Figure 3.

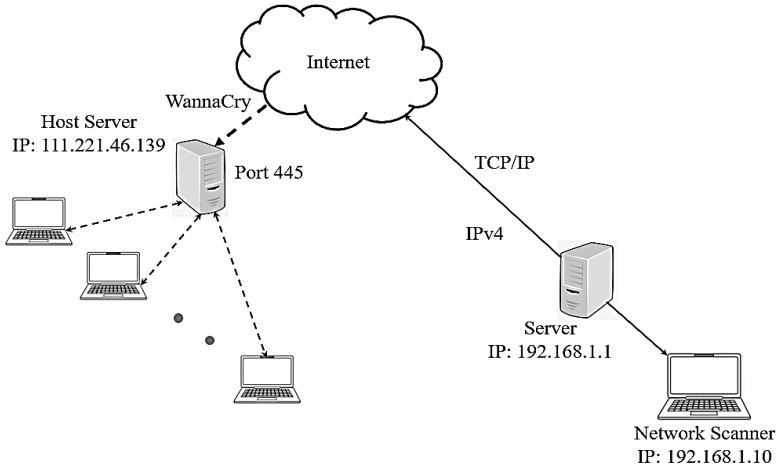


Figure 3. Testbed for scenario planning model

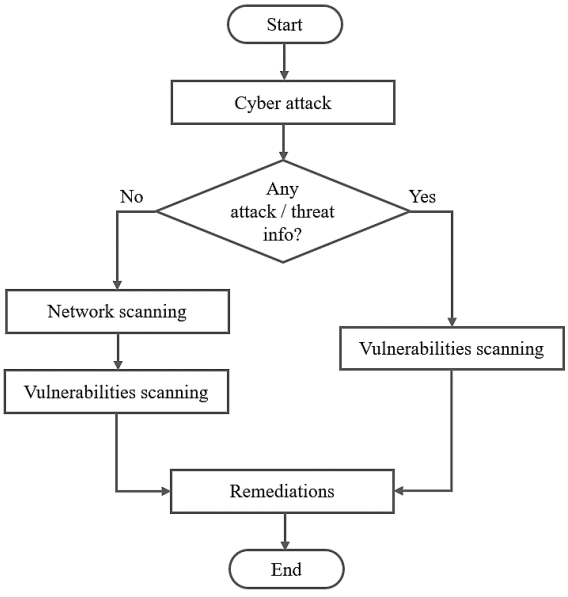


Figure 4. Simulation flow chart of vulnerability scanning with conditions 1 and 2

For condition 1, there is no malware character information. Therefore, the first action that must be done is a network scan by searching for open ports on the target IP address. Furthermore, vulnerability scanning is carried out by identifying services on open ports. Finally, the vulnerability scan results are followed up with remediation to block or activate the filter (firewall). For condition 2, information about the character of the malware is known, and vulnerability scanning can be performed immediately. For example, WannaCry malware exploits the EternalBlue leaks, explicitly attacking the system via ports 139 and 445. Therefore, vulnerability scans are directed to those ports. Furthermore, the scan results are followed up with remediation to block or activate the filter (firewall).

In the simulation, open port search tests are conducted at one IP address (111.221.46.139). And then identify vulnerabilities in open ports based on the version information of the program used by that port. The scan was carried out with the Nmap application. In Zmap and Masscan, unable to perform multi-port scanning on only one IP address. In addition, Zmap and Masscan do not provide a command line that can detect port vulnerabilities by identifying services, versions, and operating systems or firewalls [25], [26].

3. RESULTS AND DISCUSSION

This section describes the results of the experiments, from benchmarking testing and scenario planning to a simulation with two previous conditions. At first, the implementations of three network scanners are carried out according to the flow chart. Then, the experiment goes: i) to prepare the operating system and three scanning applications for the experiment: Nmap, Zmap and Masscan. All applications run on the internet on the Kali Linux operating system with a 10 Mbps IPv4 protocol. VirtualBox is used for virtualization on Windows 10. Virtualization programs and operating systems run first; ii) to run three scanning applications with the same number of target hosts, 256 ports with port lookups on port 80-the scan arguments for each application as in Figure 5; and iii) to collect the result data from 10 test attempts for each scanning application. For each variable, accuracy and response time are accumulated and then averaged. The samples of scanning results for Nmap, Zmap and Masscan are shown in Figures 6(a), 6(b) and 6(c), respectively. The results are listed in Tables 2, 3 and 4 as well.

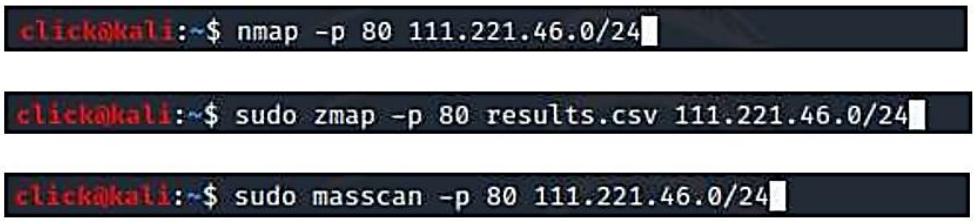
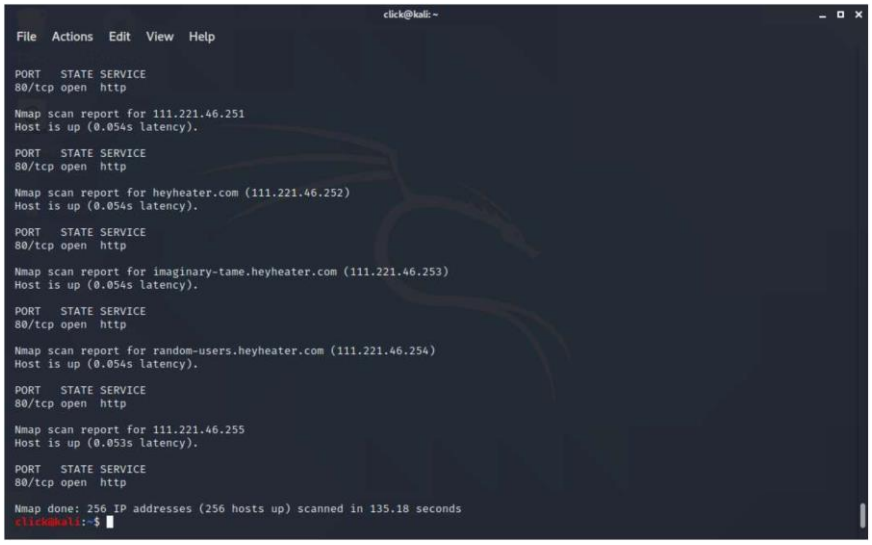


Figure 5. Command-line from Nmap, Zmap, and Masscan

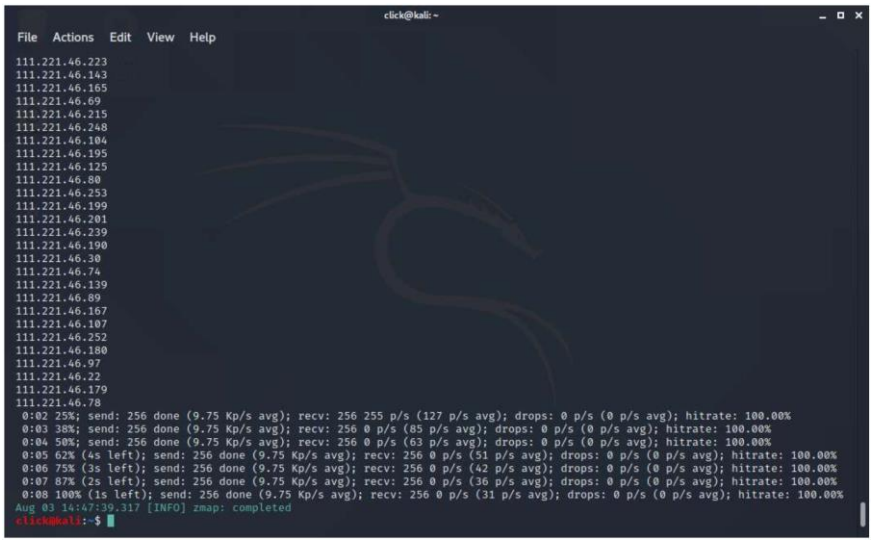
In the condition 1 case simulation, a network scanning is conducted with the target of all ports on the host with IP address 111.221.46.139. The task is to find open ports. The process is done because the information about the character of the malware that attacks is not yet known. The tests were carried out ten times. From the results of vulnerability scanning on open ports with the IP address 111.221.46.139, which identified application versions, it was found that 12 ports had vulnerabilities. This scan needs to be followed up with remediation to block or activate a filter (firewall).

For the second case simulation, the malware information from the third party is known. The attack has been identified as WannaCry, malware-type ransomware which can block systems or delete information on the system [17]. This malware takes advantage of a vulnerability in EnternalBlue, a piece of software to exploit stolen and leaked cyberattacks. The WannaCry character attacks specific ports on the system, namely ports 139 and 445. In this case simulation, a vulnerability scan was performed directly to these ports with the target IP address 111.221.46.139.

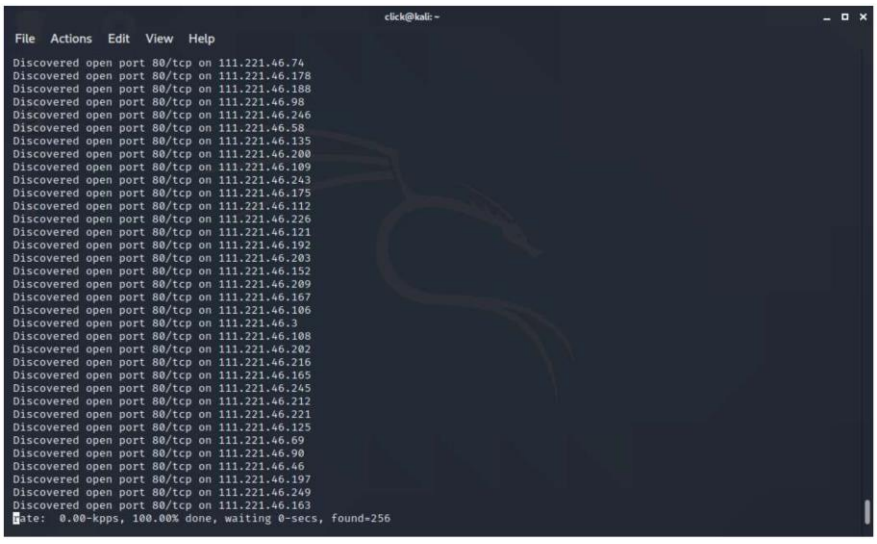
Comparing scanning Nmap with Zmap and Masscan is impossible since Zmap and Masscan do not provide a comprehensive port scanning function on only one IP address by determining the port number first. Zmap and Masscan cannot do port scanning on a target IP address without specifying the port first. The command line for this type of scan does not exist in Zmap and Masscan. In addition, Zmap and Masscan do not provide a command line to identify vulnerabilities on ports, either by the version, operating system, or firewall.



(a)



(b)



(c)

Figure 6. Sample of scanning results (a) Nmap, (b) Zmap, and (c) Massccan

Table 2. Scanning results with Nmap

No.	Scanning Results	Response Time (second)	Accuracy (%)
1	Nmap done: 256 IP address (256 host up) scanned	338.65	100
2	Nmap done: 256 IP address (256 host up) scanned	338.54	100
3	Nmap done: 256 IP address (256 host up) scanned	340.96	100
4	Nmap done: 256 IP address (256 host up) scanned	338.63	100
5	Nmap done: 256 IP address (256 host up) scanned	338.61	100
6	Nmap done: 256 IP address (256 host up) scanned	338.85	100
7	Nmap done: 256 IP address (256 host up) scanned	338.66	100
8	Nmap done: 256 IP address (256 host up) scanned	338.60	100
9	Nmap done: 256 IP address (256 host up) scanned	338.65	100
10	Nmap done: 256 IP address (256 host up) scanned	338.66	100

Table 3. Scanning results with Zmap

No.	Start Time	End Time	Response Time (second)	Accuracy (%)
1	10:38:59.122	10:39:08.140	9.018	100
2	10:43:18.348	10:43:27.363	9.015	100
3	10:46:08.226	10:46:17.241	9.015	100
4	10:48:02.344	10:48:11.357	9.013	100
5	10:49:13.600	10:49:22.618	9.018	100
6	10:50:34.823	10:50:43.838	9.015	100
7	10:51:41.407	10:51:50.425	9.018	100
8	10:52:43.605	10:52:52.621	9.016	100
9	10:53:51.736	10:54:00.752	9.016	100
10	10:54:55.906	10:55:04.920	9.014	100

Table 4. Scanning results with Masscan

No.	Scanning Results	Response Time (second)	Accuracy (%)
1	Scanning 256 hosts [1 port/host]	3,000	100
2	Scanning 256 hosts [1 port/host]	2,000	100
3	Scanning 256 hosts [1 port/host]	1,000	100
4	Scanning 256 hosts [1 port/host]	2,000	100
5	Scanning 256 hosts [1 port/host]	2,000	100
6	Scanning 256 hosts [1 port/host]	1,000	100
7	Scanning 256 hosts [1 port/host]	1,000	100
8	Scanning 256 hosts [1 port/host]	2,000	100
9	Scanning 256 hosts [1 port/host]	2,000	100
10	Scanning 256 hosts [1 port/host]	1,000	100

In this section, the overall results of the experiment were analyzed. Based on the test results with the benchmarking model, out of 10 trials, the three network scanning applications have an average accuracy of 100%. Furthermore, Masscan achieves the fastest response time than Zmap and Nmap, as listed in Table 5. The results of benchmarking tests can be used to compare these three scanning techniques and confirm what happened in the experiment with what was written in the literature [5]. Furthermore, even if not run with high specification computer and bandwidth for large-scale Internet scanning, the Zmap and Masscan applications are consistently fast scanning [25], [26]. According to de Santis [12] research, network scanning applications have high accuracy. The port scanning accuracy rate in the benchmarking test study is 100% in all experiments. However, various response time differences are possible because the scanning application communication with ports has a different approach.

Table 5. Benchmarking test results for three network scanners

No.	Scanners	Accuracy	Response Time (seconds)
1	Nmap	100%	338,881
2	Zmap	100%	9,016
3	Masscan	100%	1,700

In Nmap, the port scanning technique is done by relating the ports one by one with three-way handshaking, which causes the process to take a long time. However, Nmap has more detailed reports [27], [28]. Even when using a technique similar to Nmap's of addressing ports individually, Zmap outperforms Nmap by up to 38 times in this experiment. Furthermore, ZMap uses a cyclic multiplication group technique to communicate with the scanning target. The process allows ZMap to scan approximately 1,300 times faster than Nmap [25]–[28].

In benchmarking tests, Masscan was the fastest. Response times are up to 200 times faster than Nmap. This is because Masscan communicates with the scanning target ports simultaneously, not individually. In addition, Masscan uses a custom TCP/IP stack communication technique. With a quad-core processor and 10 Gbps bandwidth, Masscan can transmit 25 million packets per second, scanning large-scale internet networks with a response time of fewer than 3 minutes [29]. In the case of simulation experiments, scenario planning models can be implemented. This model was chosen to evaluate the port scanning of the host in anticipation of uncertain conditions due to cyber-attacks, while the problem must be resolved immediately [30]. For condition 1, two scanning stages are needed, each of which takes longer than condition 2. This time difference is very tactical when facing an attack. The sooner a vulnerability is discovered, the sooner effective network security protection is implemented. So that damage to the system can be stopped or avoided.

In simulation tests, scenario planning models can be implemented. The model was chosen to evaluate the port scanning of the host in anticipation of uncertain conditions due to cyber-attacks, while the problem must be resolved immediately [31]–[33]. For condition 1, two scanning types need to be conducted, therefore taking longer than in condition 2. This time difference is very tactical when facing an attack. The sooner a vulnerability is discovered, the sooner effective network security protection is implemented. So that damage to the system can be stopped or mitigated. From the two conditions in the scenario, there is two response time gap that is much different. In condition 2, given the initial information, the scan can be conducted with a response time of 3.89 seconds. In condition 1, the scan obtains a longer response time of 1,374,31 seconds. Vulnerabilities scanning steps in condition 1 can be avoided by continually updating the information about the character of the cyber-attack. To get to know the target ports, as shown in Table 6.

Table 6. Scanning test results of scenario planning model

	Condition 1	Condition 2
Response time (seconds)	1,374,31	3.89

From the scanning results of the two test models, the response time optimization can be obtained. Based on benchmarking three scanning techniques for open port search on network subnets, Masscan can do less than 2 seconds (1.70 seconds) and, based on scenario planning for vulnerability detection on one host by Nmap scanning, can achieve optimal results in less than 4 seconds (3.89 seconds). The total accumulated response time of the two test models was less than 6 seconds (5.59 seconds). Therefore, combining the benchmarking model with scenario planning can optimize effective response time.

4. CONCLUSION

Based on testing with the benchmarking model, network scanning to search the open port on the subnet, from the three scanning techniques (Nmap, Zmap, and Masscan), all experiments yield 100% accuracy. The fastest is Masscan, with response times of less than 2 seconds. Vulnerability scanning tests with multiple ports target one IP address without first indicating the port number, and only Nmap can conduct. Based on testing with a scenario planning model, vulnerability scanning will be more effective if preliminary information about malware attacks ports target is known. The case simulation in condition 2 shows that the response time is faster than condition 1, less than 4 seconds. In this research, vulnerability scanning tests have been carried out using some scanning techniques. By combining the benchmarking and scenario planning model, an effective, optimized response time can be obtained, accumulating the scan results of both test models. The total response time achieved is less than six seconds.

ACKNOWLEDGEMENTS

The authors would like to thank the financial support from the Directorate General of Higher Education, Ministry of Education and Culture of the Republic of Indonesia for the Master's Research Scheme No. B/87/E3/A.00/2020. Countless greetings to the Universitas Mercu Buana Research Centre for their support and encouragement.

REFERENCES

[1] J. M. Couretas, "Cyber security and defense for analysis and targeting," in *An Introduction to Cyber Analysis and Targeting*, Cham: Springer International Publishing, 2022, pp. 119–150.

[2] D. Kant and A. Johannsen, "Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs)," *Electronic Imaging*, vol. 34, no. 3, pp. 1–8, Jan. 2022, doi: 10.2352/EI.2022.34.3.MOBMU-387.
[3] A. Shahab, M. Nadeem, M. Alenezi, and R. Asif, "An automated approach to fix buffer overflows," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 3777–3787, Aug. 2020, doi: 10.11591/ijece.v10i4.pp3777-3787.
[4] M. I. Jambak, A. S. Mohruni, M. I. Jambak, and E. Suherman, "The process mining method approach to analyze users' behavior of internet in the local area network of Sriwijaya University," *Sinergi*, vol. 26, no. 2, May 2022, doi: 10.22441/sinergi.2022.2.003.
[5] J. M. Kizza, *Guide to computer network security*. Springer International Publishing, 2017.
[6] ITU, "World Telecommunication/ICT Indicators Database 2021," *International Telecommunication Union*, 2021.
[7] T. Yang, B. Hou, Z. Cai, K. Wu, T. Zhou, and C. Wang, "6Graph: A graph-theoretic approach to address pattern mining for Internet-wide IPv6 scanning," *Computer Networks*, vol. 203, Art. no. 108666, Feb. 2022, doi: 10.1016/j.comnet.2021.108666.
[8] S.-J. Chen, Y.-C. Pan, Y.-W. Ma, and C.-M. Chiang, "The impact of the practical security test during the software development lifecycle," in *2022 24th International Conference on Advanced Communication Technology (ICACT)*, Feb. 2022, pp. 313–316, doi: 10.23919/ICACT53585.2022.9728868.
[9] R. Haecki *et al.*, "How to diagnose nanosecond network latencies in rich end-host stacks," in *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*, 2022, pp. 861–877.
[10] R. Sabillon, "Audits in cybersecurity," in *Research Anthology on Business Aspects of Cybersecurity*, IGI Global, 2022, pp. 1–18.
[11] M. S. Vidya and M. C. Patil, "Reviewing effectivity in security approaches towards strengthening internet architecture," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3862–3871, Oct. 2019, doi: 10.11591/ijece.v9i5.pp3862-3871.
[12] R. Muwardi, H. Gao, H. U. Ghifarsyam, M. Yunita, A. Arrizki, and J. Andika, "Network security monitoring system via notification alert," *Journal of Integrated and Advanced Engineering (JIAE)*, vol. 1, no. 2, pp. 113–122, Nov. 2021, doi: 10.51662/jiae.v1i2.22.
[13] F. Sirait, A. W. Dani, Y. Yuliza, and U. Albab, "Optimization in quality of service for LTE network using bandwidth expansion," *Sinergi*, vol. 23, no. 1, Feb. 2019, doi: 10.22441/sinergi.2019.1.007.
[14] S. Lagraa and J. Francois, "Knowledge discovery of port scans from darknet," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, May 2017, pp. 935–940, doi: 10.23919/INM.2017.7987415.
[15] S. Lagraa, Y. Chen, and J. François, "Deep mining port scans from darknet," *International Journal of Network Management*, vol. 29, no. 3, May 2019, doi: 10.1002/nem.2065.
[16] M. Niedermaier, F. Fischer, D. Merli, and G. Sigl, "Network scanning and mapping for IIoT edge node device security," in *2019 International Conference on Applied Electronics (AE)*, Sep. 2019, pp. 1–6, doi: 10.23919/AE.2019.8867032.
[17] G. De Santis, "Modeling and recognizing network scanning activities with finite mixture models and hidden Markov models," Universite de Lorraine, 2018.
[18] M. O. Kalinin, "Application of neuro-fuzzy inference to detect network scanning," *Automatic Control and Computer Sciences*, vol. 55, no. 8, pp. 908–917, Dec. 2021, doi: 10.3103/S0146411621080150.
[19] E. S. Sagatov, S. Mayhoub, A. M. Sukhov, F. Esposito, and P. Calyam, "Proactive detection for countermeasures on port scanning based attacks," in *2021 17th International Conference on Network and Service Management (CNSM)*, Oct. 2021, pp. 402–406, doi: 10.23919/CNSM52442.2021.9615577.
[20] Q. Gong and C. Gu, "A Baseline modeling algorithm for internet port scanning radiation flows," in *2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP)*, Oct. 2021, pp. 1255–1259, doi: 10.1109/ICSIP52628.2021.9688791.
[21] T. Yang *et al.*, "Formal analysis of 5G authentication and key management for applications (AKMA)," *Journal of Systems Architecture*, vol. 126, May 2022, doi: 10.1016/j.sysarc.2022.102478.
[22] R. Graham, "Masscan: Mass IP port scanner," Github.com, 2022. Accessed: Feb. 1, 2022. [Online]. Available: https://github.com/robertdavidgraham/masscan.
[23] A. Tanaka, C. Han, T. Takahashi, and K. Fujisawa, "Internet-wide scanner fingerprint identifier based on TCP/IP header," in *2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC)*, Dec. 2021, pp. 1–6, doi: 10.1109/FMEC54266.2021.9732414.
[24] J. Patil, V. Tokekar, A. Rajan, and A. Rawat, "Port scanning based model to detect malicious TCP traffic and mitigate its impact in SDN," in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, May 2021, pp. 365–370, doi: 10.1109/ICSCCC51823.2021.9478150.
[25] M. Akbanov, V. G. Vassilakis, I. D. Moscholios, and M. D. Logothetis, "Static and dynamic analysis of WannaCry ransomware," *Proc. IEICE Inform. and Commun. Technol. Forum ICTF 2018*, 2018.
[26] Z. Li, J. Xiao, X. Han, and W. Zhang, "Z-map based cutting force prediction for elliptical ultrasonic vibration-assisted milling process," *The International Journal of Advanced Manufacturing Technology*, vol. 120, no. 5–6, pp. 3237–3249, Mar. 2022, doi: 10.1007/s00170-022-08976-w.
[27] Z. Zhang, D. Towey, Z. Ying, Y. Zhang, and Z. Q. Zhou, "MT4NS: metamorphic testing for network scanning," in *2021 IEEE/ACM 6th International Workshop on Metamorphic Testing (MET)*, Jun. 2021, pp. 17–23, doi: 10.1109/MET52542.2021.00010.
[28] K. Chhillar and S. Shrivastava, "University computer network vulnerability management using Nmap and Nexpose," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, no. 6, pp. 3084–3090, Dec. 2021, doi: 10.30534/ijatcse/2021/021062021.
[29] K. Kumar and M. Khari, "Architecture of digital twin for network forensic analysis using Nmap and Wireshark," in *Digital Twin Technology*, Boca Raton: CRC Press, 2021, pp. 83–104.
[30] S. Alazmi and D. C. De Leon, "A systematic literature review on the characteristics and effectiveness of web application vulnerability scanners," *IEEE Access*, vol. 10, pp. 33200–33219, 2022, doi: 10.1109/ACCESS.2022.3161522.
[31] C. Liu, S. Hao, Q. Liu, C. Bao, and X. Li, "IPv6-network telescope network traffic overview," in *2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Jun. 2021, pp. 1–4, doi: 10.1109/ICEIEC51955.2021.9463724.
[32] KALI, "Kali tools." Accessed: March. 10, 2022. [Online]. Available: https://www.kali.org/tools/.
[33] T. R. Fakhrurrasi, A. Adriansyah, S. Budiyanto, J. Andika, S. Haryanti, and U. A. Rachmawati, "Load balance optimization in peer classifier robin method as hybrid from peer connection classifier and round robin methods," *Journal of Engineering Science and Technology*, vol. 16, no. 3, pp. 2528–2543, 2021.

BIOGRAPHIES OF AUTHORS

Arif Basuki graduated with his Bachelor in Electrical Engineering from the Faculty of Engineering, University of Indonesia, majoring in Telecommunication Engineering in 1995. After that, he graduated from the Post Graduate School of Electrical Engineering at Mercu Buana University. After that, he became an engineer at Telecommunication Solutions, Multimedia Global Wagon, Jakarta, Indonesia. From 1995-now, he has worked at some telecommunication enterprises in Indonesia and abroad, such as Jeddah, KSA, New Jersey, US and Dubai, and Uni Emirat Arab. He can be contacted at email: arifbsk@yahoo.com.

Andi Adriansyah is a professor in Electrical Engineering in Universitas Mercu Buana born in 1970. He completed his undergraduate education in Electrical Engineering Universitas Indonesia, Indonesia, in 1994. Then, his master's and doctoral education were completed at Universiti Teknologi Malaysia, Malaysia, in 1998 and 2007, respectively. In addition, he conducts some research in mechatronics, robotics, control and automation, artificial intelligence, and the internet of things (IoT). He can be contacted at email: andi@mercubuana.ac.id.