Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 9, No. 2, June 2023, pp. 375-384
ISSN: 2338-3070, DOI: 10.26555/jiteki.v9i2.26167

Descriptive Analysis and ANOVA Test with File Sending on Computer Networks Attacked with Rogue's Dynamic Host Configuration Protocol (DHCP)

Hero Wintolo [1], Yuliani Indrianingsih [2], Wahyu Hamdani [3], Syafrudin Abdie [4]
[1,2,3] Informatika, Institut Teknologi Dirgantara Adisutjipto
[4] Teknik Elektro, Institut Teknologi Dirgantara Adisutjipto

ARTICLE INFO

Article history:

Received April 04, 2023
Revised May 25, 2023
Published May 27, 2023

Keywords:

Descriptive Analysis;
Nova Test;
Networks Attacked;
DHCP Rogue

ABSTRACT

The requirement for a computer that is physically connected to a computer network is to be able to access existing resources on a computer network in the form of an IP address obtained statically or dynamically. On a static IP address, there are not many problems that arise because it is loaded directly into the computer, while for a dynamic IP address, security problems arise in the form of a dynamic IP address sharing server in the form of DHCP Rogue. The contribution of this research is to detect attacks on a computer network and specifically to find out which computer networks are affected by DHCP rouge-type attacks. The configuration that is added to the first router when the network is hit by a DHCP rogue attack is to configure the main router, in this case, the first router, and the switch used as a connecting device between computers. configuration on both switches is done by snooping trust which is useful for securing IP addresses to avoid IP attackers. This research was conducted to find out if a computer network with a dynamic IP address was attacked by sending files between computers. Files with the longest sending time indicate an attack on the computer network. The method used in this study is the ANOVA test with descriptive-based analysis. Based on the results of the analysis, it is known that the average file transfer time on networks affected by DHCP Rogue is higher than the average file transfer time on normal and mitigated networks, and the significant value of the ANOVA test results has a value of 0.004. In general, it can be concluded that there are differences in data transfer when the network is normal, the network is subject to DHCP Rogue, and the network has been mitigated with DHCP Rogue.

Corresponding Author:

Hero Wintolo, Institut Teknologi Dirgantara Adisutjipto, Jl. Majapahit, Blok-R, Lanud Adisucipto, Yogyakarta, 55198, Indonesia
Email: herowintolo@itda.ac.id

1. INTRODUCTION

Computers that are connected physically or non-physically with computer networks are very vulnerable to interference from within and from outside. Physically a computer connected to a computer network requires transmission media and end devices. Non-physical computers connected to a computer network must have an address known as an IP address. This address is entered into the computer in two ways, the first is entered manually into the computer, and the second way is filled in by software that can be placed on a server or router in charge of providing the address, which is known as the Dynamic Host Configuration Protocol (DHCP), DHCP server can be applied to wireless router equipment [1], DHCP can also be implemented on a wireless network [2], On a wireless network, the DHCP configuration process can use Behavior-aware Dynamic Adaptive Configuration (BDCA) [3] and DHCP can also support internet networks from Internet Service

Providers within 24 hours per week [4]. To secure DHCP when sharing IP can use OTP [5]. IP address assignment using DHCP can be arranged to reduce DHCP overhead [6].

DHCP is very vulnerable to interference and attacks, which will result in the provision of IP address services to computers connected to computer networks being disrupted. Security disturbances in computer networks can be monitored using wire shark software [7]–[10] Snort Intrusion Detection System (IDS) [11], [12], in terms of access points can use the vemos D1 microcontroller [13] and use the round trip time method [14]. In DHCP, security breaches can also occur in the form of starvation [15], spoofing [16], malicious DHCP client attacks, and rouge [17], DHCP attack analysis in the form of flooding and starvation can be done using a novel technique [18]. DHCP rouge can be detected using DHCP snooping [19],[20] which is legal software placed on routers, servers, and access points. Monitoring and detection are needed to secure computer networks from various kinds of attacks, but preventing attacks is also very necessary, DHCP security can be done with AC Address Whitelist Authentication and DHCP Fingerprint Recognition [21]. DHCP that can be used to prevent attacks on computer networks, namely SDHCP, provides IP address recovery services by placing a distributed DHCP Server [22] and can also use a Virtual Local Area Network (VLAN) [23]. Prevention of attacks on computer networks can also be done by applying cryptographic techniques [24]. DHCP attack detection can be detected using a program made in Python [25]. How to detect DHCP rouge by creating an algorithm on the Linux operating system [26]. DHCP starvation detection can be performed with Software Defined Networking [27]. Identification of DHCP attacks can be done by combining ICMP and ARP [28]. Examination of computer networks affected by DHCP snooping can be carried out using SSL stripping techniques [29]. Attack detection against DHCP can also be performed with the Measurement inconsistent discrete event system (MIDES) [30].

Computers that are affected by DHCP routing interference will get a different IP address from computers that are not affected by the interference so that these computers cannot communicate with other computers in the computer network. Detect processes on computer networks that have not been and have been hit by DHCP rogue attacks by using file transfers between computers. Computer delivery speed data will be analyzed using descriptive and ANOVA tests [31], descriptive analysis has also been used for Micro, Small, and Medium Enterprises (MSMEs) [32], the Fintech Industry in Indonesia [33], and e-commerce [34]. The ANOVA test, also known as the F test for MSMEs [35] has been used in performance speed [36], reasoning ability [37], defining pixels[38], and machine learning [39], [40]. Research on networks affected by DHCP rouge attacks by utilizing computers on the network to send files to each other whose speed data is analyzed descriptively and an ANOVA test has never been done. This research is specifically to investigate DHCP Rouge attacks on a computer network, the method used to investigate by sending files between computers and the time required for sending is analyzed, this has never been done before

2. METHODS

The research process to be carried out is illustrated using a flow chart which can be seen in Fig. 1. The initial stage of research is the identification stage or the beginning to be able to deal with certain problems or conditions. The systems requirements stage is divided into 3 points which will be described, namely hardware and software specifications, and research data needs. The system design stage is the stage of making software used for sending files and recording the time needed. After the software is complete, the next step is data collection. The data collected is in the form of speed in sending files between computers which will then be analyzed in the next stage.

Our research has a hypothesis. namely that there are striking differences in data transfer on normal networks, being attacked and mitigated. So, it can be formulated to prove whether there is a difference during data transfer, namely:

1. Ho: There is no difference from data transfer when the network is normal, the network is exposed to DHCP Rogue, and the network has been mitigated from DHCP Rogue performed to 30 clients using a Cisco Router 2800.
2. Ha: There is a difference from data transfer when the network is normal, the network is exposed to DHCP Rogue, and the network has been mitigated from DHCP Rogue performed to 30 clients using a Cisco Router 2800.

The network topology used in this research is to use 30 computers as clients who will receive file transfers from the computer server. The task of the server computer is to transfer files to the client. All computers, both client and server, are connected to form a LAN network using 2 switches. Then two routers, one acts as DCHP, and the other acts as a router to provide fake DHCP addresses to clients as shown in Fig. 2.

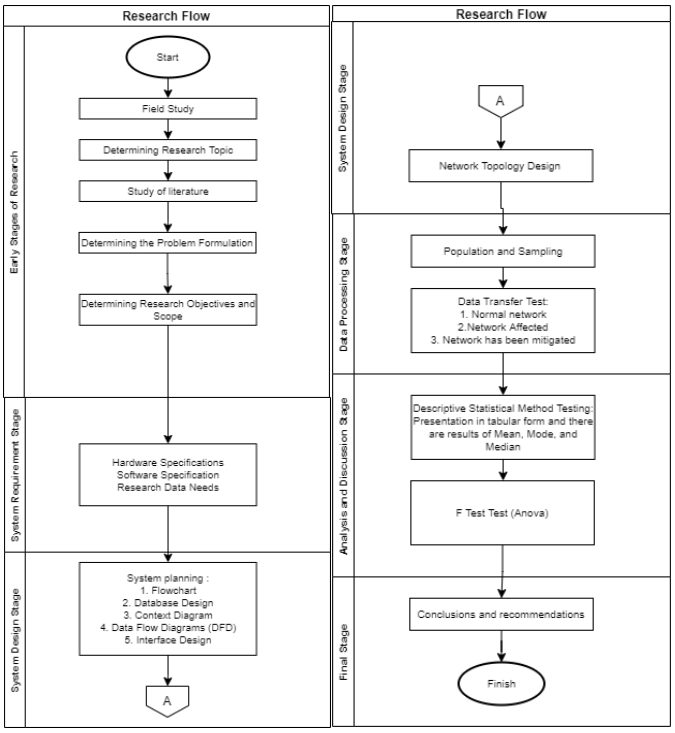

Fig. 1. Research diagram

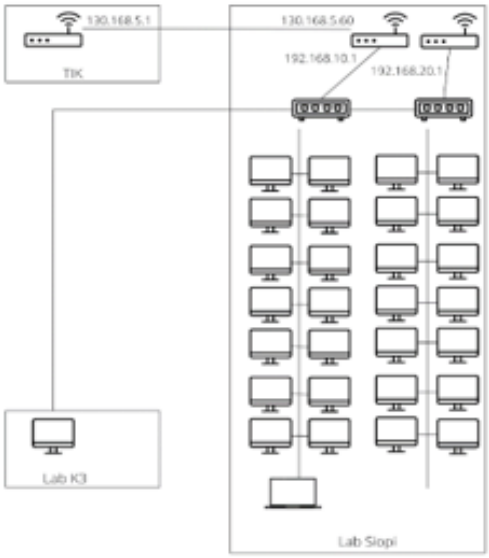

Fig. 2. Network Topology Design

3. RESULT AND DISCUSSION

The results of this research are in the form of software used to upload files and analyzed the results of uploading. In Fig. 3, files are uploaded via the server computer to 30 client computers. The statistic page provides information about the files transferred and how many users received the files. This page will automatically move when pressing the transfer button on the file upload page.

Something that must be prepared before testing the software is the Router configuration. The configuration carried out on this router is the configuration of the IP address on the Router port and the DHCP configuration. This Router has 2 ports, namely fastethernet0/0 and *fastethernet0/1*. Each port is used to connect

to other devices using a LAN cable. Fastethernet0/1 port is configurated with IP address 192.168.10.1 and subnetfastethernet0/1.mask.255.255.255.0. The results of this configuration are IP addresses on 30 client computers that are filled automatically with results as shown in Table 1.

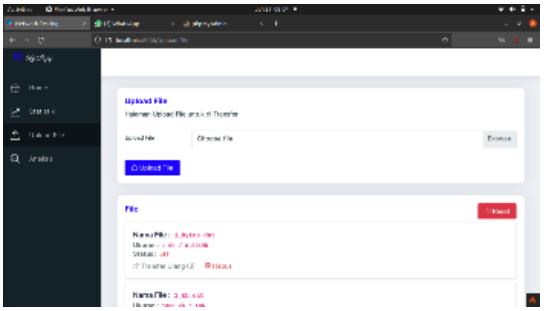

Fig. 3. Tested Research Software

Table 1. IP address Configuration Display

No.	Computer Name	IP Address	Subnet Mask
1.	Client 1	192.168.10.31	255.255.255.0
2	Client 2	192.168.10.21	255.255.255.0
3	Client 3	192.168.10.20	255.255.255.0
4	Client 4	192.168.10.19	255.255.255.0
5	Client 5	192.168.10.17	255.255.255.0
6	Client 6	192.168.10.18	255.255.255.0
7	Client 7	192.168.10.16	255.255.255.0
8	Client 8	192.168.10.2	255.255.255.0
9	Client 9	192.168.10.13	255.255.255.0
10	Client 10	192.168.10.8	255.255.255.0
11	Client 11	192.168.10.6	255.255.255.0
12	Client 12	192.168.10.5	255.255.255.0
13	Client 13	192.168.10.22	255.255.255.0
14	Client 14	192.168.10.3	255.255.255.0
15	Client 15	192.168.10.24	255.255.255.0
16	Client 16	192.168.10.9	255.255.255.0
17	Client 17	192.168.10.7	255.255.255.0
18	Client 18	192.168.10.10	255.255.255.0
19	Client 19	192.168.10.11	255.255.255.0
20	Client 20	192.168.10.12	255.255.255.0
21	Client 21	192.168.10.14	255.255.255.0
22	Client 22	192.168.10.15	255.255.255.0
23	Client 23	192.168.10.4	255.255.255.0
24	Client 24	192.168.10.27	255.255.255.0
25	Client 25	192.168.10.28	255.255.255.0
26	Client 26	192.168.10.29	255.255.255.0
27	Client 27	192.168.10.30	255.255.255.0
28	Client 28	192.168.10.26	255.255.255.0
29	Client 29	192.168.10.25	255.255.255.0
30	Client 30	192.168.10.23	255.255.255.0

After configuring and transferring data for 4 file types, namely 1 Byte, 1 KB, 1 MB, and 1 GB on a normal network (Normal) or has not been hit by a DHCP rouge attack. Then the network is subjected to a DHCP rouge attack by setting the second router to be configured so that several client computers have different network addresses. On networks affected by DHCP Rogue, the configuration on the router is almost the same as the configuration on the main router but only uses 1 port to be connected to the switch, namely the fastethernet0/1 port configured with an IP address of 192.168.20.1 and subnet mask of 255.255.255.0. The configuration is as follows:

1. Router>enable
2. Router#configure terminal
3. Router (config) # interface fastEthernet 0/1

4. Router (config-if) #ip address 192.168.20.1 255.255.255.0
5. Router (config-if) #no shutdown
6. Router (config-if) #exit the rout
7. Router (config) #ip dhcp pool net2
8. Router (dhcp-config) #network 192.168.20.0 255.255.255.0
9. Router (dhcp-config) #default-router 192.168.20.1
10. Router (dhcp-config) #exit
11. Router (config) #ip dhcp exclude-address 192.168.20.7 192.168.20.254

The display of the IP address affected by the attack is different from the IP address given by the main router, the main router provides an IP with network 192.168.10.0, while the IP from the attacker router has *Network* 192.168.20.0. Table 2 shows the IP addresses of several computers which are the results of the configuration of the network that has been affected by DHCP Rogue.

Table 2. Display IP address After Attack

No.	Computer Name	IP Address	Subnet Mask
1	Client 7	192.168.20.5	255.255.255.0
2	Client 12	192.168.20.6	255.255.255.0
3	Client 23	192.168.20.3	255.255.255.0
4	Client 25	192.168.20.4	255.255.255.0
5	Client 30	192.168.20.2	255.255.255.0

Mitigation needs to be done by connecting devices between computers. The configuration added on the first router when the network is hit by a DHCP rouge attack is to configure the main router, in this case, the first router, and the switch that is used as a connecting device between computers. The configuration added on the first router is as follows:

1. Router>enable
2. Router#configure terminal
3. Router (config) #ip dhcp exclude-address 192.168.10.32 192.168.10.254

While the configuration on both switches is carried out by snooping trust which is useful for securing IP addresses to avoid IP attackers, The configuration on the first switch is as follows: :

1. Switch>enable
2. Switch#configure terminal
3. Switch (config) #interface fastEthernet 4/0/24
4. Switch (config-if) #switchport mode access
5. Switch (config-if) #switchport access vlan 1
6. Switch (config-if) #no shutdown
7. Switch (config-if) #exit
8. Switch (config) #ip shcp snooping
9. Switch (config) #ip dhcp snooping vlan 1
10. Switch (config) #interface fastEthernet range 4/0/1-15
11. Switch (config-if) #ip dhcp snooping trust
12. Switch (config-if) #exit

And the configuration on the second switch is as follows:

1. Switch>enable
2. Switch#configure terminal
3. Switch (config) #interface fastEthernet 5/0/24
4. Switch (config-if) #switchport mode access
5. Switch (config-if) #switchport access vlan 1
6. Switch (config-if) #no shutdown
7. Switch (config-if) #exit
8. Switch (config) #ip dhcp snooping
9. Switch (config) #ip dhcp snooping vlan 1
10. Switch (config) #interface fastEthernet range 5/0/1-15
11. Switch (config-if) #ip dhcp snooping trust
12. Switch (config-if) #exit

After configuring and transferring data for 4 file types, namely 1 Byte, 1 KB, 1 MB, and 1 GB on a normal network (Normal), a network that is attacked by DHCP Rogue (Attack), and a network that has been mitigated from DHCP Rogue (Repair) then the results are as shown in Table 3, with N as normal or the network in an unattended state, A as an attack, i.e. the network is under attack using DHCP rouge and R as repair, i.e. when the attacked network is subjected to mitigation, these three conditions has units of milliseconds (ms). The result of the data transfer has a N/A value which means that the data has been sent but did not arrive at the destination so it has a value of 10800000 ms (3 hours) as a replacement.

Table 3. Transfer Data File On 30 Client Computers

Client No	Transfer file 1 byte			Transfer file 1 K byte			Transfer file 1 M byte			Transfer file 1 G byte		
	N	A	R	N	A	R	N	A	R	N	A	R
1	16	20	19	23	N/A	23	20	16	24	23	83	65
2	17	N/A	33	17	23	18	31	21	28	34	61	63
3	17	20	29	18	23	17	29	27	26	44	32	22
4	18	23	23	19	24	24	22	24	26	40	43	35
5	19	16	519	23	32	44	46	34	14	63	30	348
6	34	19	20	19	22	23	21	27	23	90	42	48
7	35	20	20	23	28	23	20	37	23	67	1032	41
8	49	N/A	24	44	19	34	35	27	15	90	N/A	79
9	30	25	24	20	18	22	22	29	24	85	402	51
10	56	25	23	14	18	24	20	28	40	44	N/A	98
11	39	19	21	20	N/A	714	21	21	46	31	181	59
12	18	29	24	19	20	16	21	26	25	96	81	26
13	18	19	25	23	N/A	30	31	N/A	28	113	N/A	99
14	17	N/A	26	28	21	20	25	68	38	142	85	42
15	23	16	22	20	28	23	43	49	21	57	N/A	85
16	17	21	29	20	23	19	32	42	32	72	41	41
17	19	20	20	18	25	17	44	55	24	775	N/A	72
18	20	21	33	22	29	18	25	N/A	36	94	27	36
19	21	23	20	20	20	22	24	45	33	23	29	37
20	19	36	13	32	20	23	27	57	41	115	109	83
21	21	19	15	23	N/A	32	30	40	30	41	71	29
22	22	20	18	21	21	24	26	N/A	29	94	90	40
23	22	22	15	17	19	27	26	34	24	571	94	50
24	22	21	19	21	35	15	23	39	22	54	39	38
25	21	N/A	26	25	21	21	20	N/A	22	87	25	63
26	56	25	23	19	34	22	29	65	28	153	46	46
27	44	20	23	21	19	24	29	30	27	54	117	20
28	61	N/A	24	23	26	25	24	N/A	23	106	26	23
29	20	15	20	21	N/A	20	22	28	26	646	33	67
30	22	17	27	25	27	24	28	43	37	34	31	39

The results of the transfer test of 4 files with different sizes in three different circumstances were then analyzed descriptively to get the mean and median data as shown in Table 4. It can be seen that there is a slight difference between the network in a state not being attacked and the network being mitigated due to the attack, and a very big difference when the network is under attack using the DHCP route.

The next test is hypothesis testing. This test aims to determine whether there is a significant difference when transferring data to 30 clients using a Cisco 2800 Router. The basis for decision-making is if the significant value is 0.05, then Ho is accepted, while if the significant value is 0.05, then Ho is rejected. Ho: there is no difference in data transfer when the network is normal, the network is under DHCP Rogue, and the network has been mitigated from DHCP Rogue performed on 30 clients using a Cisco 2800 Router. Ha: there is a difference from data transfer when the network is normal, the network is DHCP Rogue and the network has been mitigated from DHCP Rogue performed on 30 clients using a Cisco 2800 Router.

Table 4. Descriptive Analysis Results

		Normal	Attack	Repair
N	Valid	30	30	30
	Missing	0	0	0
Mean		27.10	1800017.70	39.23
Std. Error of Mean		2,434	747407,849	16,566
Median		21,00	21,00	23,00
Mode		17[a]	20	20
Std. Deviation		13,332	4093721,384	90,736
Variance		177,748	1,676E+13	8233,082
Minimum		16	15	13
Maximum		61	10800000	519
Sum		813	54000531	1177

Based on the results of the analysis that has been made and then made in a table in Table 5, it can be interpreted as follows:

1. In the 1-byte file transfer test, 0.004 is significantly smaller than 0.05, so H0 is rejected.
2. In the 1 KB file transfer test, 0.004 is significantly smaller than 0.05, so H0 is rejected.
3. In the 1 KB file transfer test, 0.004 is significantly smaller than 0.05, so H0 is rejected.
4. In the 1 KB file transfer test, 0.004 is significantly smaller than 0.05, so H0 is rejected.

Table 5. Anova Test

	Anova Test			
	1 *byte*	1 KB	1 MB	1 GB
Sig.	0.004	0.004	0.004	0.004

After knowing that this application can perform data transfer and analysis, the research is continued only to find out whether this application can detect other attacks. The attack that will be tested is a DHCP Starvation Attack which is an attack on DHCP by spending all IP resources so that the client cannot receive the distributed IP. Fig. 4 shows the graphical results of descriptive statistical analysis showing the data has a value of 150, which means the data has a value greater than that value, this value is 10800000. Thus, this application is also able to determine the network affected by the DHCP Starvation Attack.

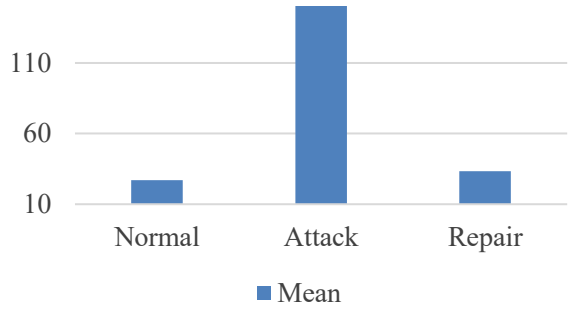

Fig. 4. Graph of Descriptive Statistics (DHCP Starvation Attack)

4. CONCLUSION

Based on the results of the study, it is known that the effect of being exposed to DHCP Rogue when data transfer is indicated by data that cannot be transferred, then the data that cannot be transferred has a value of N/A or a value of 10800000. The configuration carried out for research, to prevent the occurrence of DHCP Rogue, a Snooping configuration is carried out Trust on the Switch is useful for securing the switch using the IP Address that is used to avoid fake IPs. Calculations performed on 2 applications, namely the application created and the SPSS application, show that there is a very high difference in the value of the data transfer test when the network is exposed to DHCP Rogue than the normal network or the network that has been mitigated. The application used for data transfer and data analysis in this study can perform data transfer and also data analysis on networks affected by other attacks such as DHCP Starvation Attacks. For network managers, this

research is very useful for preventive actions needed for handling based on the time it takes for files to be received from the sending computer to the receiving computer.

REFERENCES

[1] W. A. Syafei, Y. A. A. Soetrisno, and A. B. Prasetijo, "Simple Smart Algorithm for Flexibility of Dynamic Allocation in DHCP Server for SOHO Wireless Router," in *CENIM 2020 - Proceeding: International Conference on Computer Engineering, Network, and Intelligent Multimedia 2020*, pp. 321–325, 2020, https://doi.org/10.1109/CENIM51130.2020.9297852.

[2] H. Wang *et al.*, "Squeezing the Gap: An Empirical Study on DHCP Performance in a Large-Scale Wireless Network," *IEEE/ACM Transactions on Networking*, vol. 28, no. 2, pp. 832–845, 2020, https://doi.org/10.1109/TNET.2020.2971551.

[3] C. Miao *et al.*, "BDAC: A Behavior-aware Dynamic Adaptive Configuration on DHCP in Wireless LANs," *2019 IEEE 27th International Conference on Network Protocols (ICNP)*, pp. 1-11, 2019, https://doi.org/10.1109/ICNP.2019.8888048.

[4] N. A. N. Ginarsa, P. K. Sudiarta, and W. Setiawan, "DHCP leases implementation for designing automatic power switching system," in *Proceedings of the 2020 27th International Conference on Telecommunications, ICT 2020*, pp. 1-5, 2020, https://doi.org/10.1109/ICOEI.2018.8553753.

[5] A. Shete, A. Lahade, T. Patil, and R. Pawar, "DHCP Protocol Using OTP Based Two-Factor Authentication," *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 136-141, 2018, https://doi.org/10.1109/ICOEI.2018.8553753.

[6] F. Li, X. Wang, J. Cao, R. Wang, and Y. Bi, "How DHCP Leases Meet Smart Terminals: Emulation and Modeling," *IEEE Internet Things J*, vol. 5, no. 1, pp. 56–68, 2018, https://doi.org/10.1109/JIOT.2017.2771219.

[7] S. Khant, A. Patel, S. Patel, N. Ganatra, and R. Patel, "Cyber Security Actionable Education during COVID19 Third Wave in India," *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM),* pp. 274-278, 2022, https://doi.org/10.1109/ICIEM54221.2022.9853091.

[8] M. Kassim, A. R. Mahmud, M. Amirullah Ramli and R. A. Rahman, "Network Analysis of Students' Online Activities via Port mirroring Switch Port Analyzer," *2022 IEEE 12th Symposium on Computer Applications & Industrial Electronics (ISCAIE),* pp. 49-54, 2022, https://doi.org/10.1109/ISCAIE54458.2022.9794504.

[9] I. K. N. A. Jaya, I. A. U. Dewi, and G. S. Mahendra, "Implementation of Wireshark Application in Data Security Analysis on LMS Website," *Journal of Computer Networks, Architecture and High Performance Computing*, vol. 4, no. 1, pp. 79–86, 2022, https://doi.org/10.47709/cnahpc.v4i1.1345.

[10] B. Dodiya and U. K. Singh, "Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise," *Int J Comput Appl*, vol. 183, no. 53, pp. 1–6, 2022, https://doi.org/10.5120/ijca2022921876.

[11] İ. Gündoüdu, A. A. Selçuk and S. özarslan, "Effectiveness Analysis of Public Rule Sets Used in Snort Intrusion Detection System," *2021 29th Signal Processing and Communications Applications Conference (SIU)*, pp. 1-4, 2021, https://doi.org/10.1109/SIU53274.2021.9477698.

[12] S. Syed, F. Khuhawar, and S. Talpur, "Machine Learning Approach for Classification of DHCP DoS Attacks in NIDS," in *HONET 2021 - IEEE 18th International Conference on Smart Communities: Improving Quality of Life using ICT, IoT and AI*, pp. 143–146, 2021, https://doi.org/10.1109/HONET53078.2021.9615392.

[13] W. Iman, "Sistem Deteksi Serangan Rogue Access Point," 2020, http://dspace.uii.ac.id/123456789/23645.

[14] C. Samuel, B. M. Alvarez, E. Garcia Ribera, P. P. Ioulianou, and V. G. Vassilakis, "Performance Evaluation of a Wormhole Detection Method using Round-Trip Times and Hop Counts in RPL-Based 6LoWPAN Networks," *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, pp. 1-6, 2020, https://doi.org/10.1109/CSNDSP49049.2020.9249612.

[15] S. Mishra and M. Chitkara, "Service Level Trust Key Encryption based Cloud Security using Starvation End-Point Encryption," *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, pp. 1-5, 2023, https://doi.org/10.1109/ICICACS57338.2023.10099816.

[16] S. Akashi and Y. Tong, "Classification of DHCP spoofing and effectiveness of DHCP snooping," in *Proceedings of the International Conference on Advances in Computer Technology, Information Science and Communications, CTISC 2019*, pp. 233–238, 2019, https://doi.org/10.5220/0008099002330238.

[17] M. Agarwal, S. Biswas, and S. Nandi, "Discrete event system framework for fault diagnosis with measurement inconsistency: Case study of rogue DHCP attack," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 3, pp. 789–806, 2019, https://doi.org/10.1109/JAS.2017.7510379.

[18] S. Syed, F. Khuhawar, S. Talpur, A. A. Memon, M. A. Luque-Nieto, and S. Narejo, "Analysis of Dynamic Host Control Protocol Implementation to Assess DoS Attacks," in *2022 Global Conference on Wireless and Optical Technologies, GCWOT 2022*, pp. 233-238, 2022, https://doi.org/10.1109/GCWOT53057.2022.9772887.

[19] H. A. S. Adjei, T. Shunhua, G. K. Agordzo, Y. Li, G. Peprah and E. S. A. Gyarteng, "SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection)," *2022 24th International Conference on Advanced Communication Technology (ICACT)*, pp. 187-193, 2022, https://doi.org/10.23919/ICACT53585.2022.9728961.

[20] D. A. Pradana and A. S. Budiman, "The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack," *IJID (International Journal on Informatics for Development)*, vol. 10, no. 1, pp. 38–46, 2021, https://doi.org/10.14421/ijid.2021.2287.

[21] W. Xie, J. Yu, and G. Deng, "A Secure DHCPv6 System Based on MAC Address Whitelist Authentication and DHCP Fingerprint Recognition," in *Proceedings - 2021 7th Annual International Conference on Network and Information Systems for Computers, ICNISC 2021*, pp. 604–608, 2021, https://doi.org/10.1109/ICNISC54316.2021.00114.
[22] L. Trombeta and N. M. Torrisi, "DHCP hierarchical failover (DHCP-HF) servers over a VPN interconnected campus," *Big Data and Cognitive Computing*, vol. 3, no. 1, pp. 1–16, 2019, https://doi.org/10.3390/bdcc3010018.
[23] D. Parfenov, L. Grishina, A. Zhigalov, and I. Bolodurina, "Research of Genetic Optimization Algorithms in the Design of VLAN," *2021 29th Telecommunications Forum (TELFOR),* pp. 1-4, 2021, https://doi.org/10.1109/TELFOR52709.2021.9653295.
[24] S. M. S. Reza *et al.*, "Salsa20 based lightweight security scheme for smart meter communication in smart grid," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 1, pp. 228–233, 2020, https://doi.org/10.12928/telkomnika.v18i1.14798.
[25] P. Shrestha and T. D. Sherpa, "Dynamic Host Configuration Protocol Attacks and its Detection Using Python Scripts," in *Proceedings of the International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering, ICECONF 2023*, pp. 1-5, 2023, https://doi.org/10.1109/ICECONF57129.2023.10084265.
[26] M. S. Makarova and A. A. Maksutov, "Methods of Detecting and Neutralizing Potential DHCP Rogue Servers," in *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021*, pp. 522–525, 2021, https://doi.org/10.1109/ElConRus51938.2021.9396106.
[27] C. Toprak, C. Turker, and A. T. Erman, "Detection of DHCP Starvation Attacks in Software Defined Networks: A Case Study," *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, pp. 636-641, 2018, https://doi.org/10.1109/UBMK.2018.8566268.
[28]]M. Yaibuates and R. Chaisricharoen, "A Combination of ICMP and ARP for DHCP Malicious Attack Identification," *2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON)*, pp. 15-19, 2020, https://doi.org/10.1109/ECTIDAMTNCON48261.2020.9090760.
[29] H. A. S. Adjei, M. T. Shunhua, G. K. Agordzo, Y. Li, G. Peprah, and E. S. A. Gyarteng, "SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection)," in *International Conference on Advanced Communication Technology, ICACT*, pp. 187–193, 2021, https://doi.org/10.23919/ICACT51234.2021.9370460.
[30] M. Agarwal, S. Biswas, and S. Nandi, "Discrete event system framework for fault diagnosis with measurement inconsistency: Case study of rogue DHCP attack," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 3, pp. 789–806, 2019, https://doi.org/10.1109/JAS.2017.7510379.
[31] F. Kabashi, H. Snopce, L. Abazi-Bexheti, and L. Shkurti, "Analysis of the Cases of Coronavirus in Prizren Region by using ANOVA and regression analysis," *2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*, pp. 1-6, 2021, https://doi.org/10.1109/INISTA52262.2021.9548645.
[32] E. K. Ocloo, E. Malcalm, and G. D. Kumar, "Exploration of Endogenous Constraints Leading to Failure of Micro Small and Medium Enterprises (MSMEs) in Developing Countries (A Case Study of Mallam, Greater Accra Region of Ghana)," *2021 International Conference on Computing, Computational Modelling and Applications (ICCMA),* pp. 115-121, 2021, https://doi.org/10.1109/ICCMA53594.2021.00027.
[33] A. Wahab, T. M. Alam, and M. M. Raza, "Usability Evaluation of FinTech Mobile Applications: A Statistical Approach," *2021 International Conference on Innovative Computing (ICIC)*, pp. 1-10, 2021, https://doi.org/10.1109/ICIC53490.2021.9691512.
[34] Z. Haiteng, L. Longteng, Y. Lei, L. Silin, and Z. Kaili, "Modeling and Analysis of Group Consumption Behavior of the Elderly under the Background of E-commerce," *2021 IEEE International Conference on Electronic Technology, Communication and Information (ICETCI),* 2021, https://doi.org/10.1109/ICETCI53161.2021.9563457.
[35] J. An, X. Dong, and X. Xie, "Analysis and Evaluation of Innovation Performance of Micro, Small and Medium-sized Technology Enterprises Based on ANN-RBF*,"2021 2nd International Conference on Computer Science and Management Technology (ICCSMT),* pp. 544-549, 2021, https://doi.org/10.1109/ICCSMT54525.2021.00107.
[36] F. Trejo and Y. Hu, "User Performance of VR-Based Tissue Dissection Under the Effects of Force Models and Tracing Speeds*," 2018 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, p. 707-708, 2018, https://doi.org/10.1109/VR.2018.8446310.
[37] D. Saxton, E. Grefenstette, F. Hill, and P. Kohli, "Analysing Mathematical Reasoning Abilities of Neural Models," *arXiv preprint arXiv:1904.01557*, 2019, https://doi.org/10.48550/arXiv.1904.01557.
[38] Y. Cheng, J. C. C. Lo, X. Qiu, B. Shieh, and S. W. Ricky Lee, "Quantum Dot Film Patterning on a Trenched Glass Substrate for Defining Pixel Arrays of a Full-color Mini/Micro-LED Display," *2020 21st International Conference on Electronic Packaging Technology (ICEPT)*, 2020, https://doi.org/10.1109/ICEPT50128.2020.9201924.
[39] D. J. Perangin-Angin and F. A. Bachtiar, "Classification of Stress in Office Work Activities Using Extreme Learning Machine Algorithm and One-way ANOVA F-Test Feature Selection," *2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI),* pp. 5-3-508, 2021, https://doi.org/10.1109/ISRITI54043.2021.9702802.
[40] R. Yusuf, *et al.*, "Comparing Different Supervised Machine Learning Accuracy on Analyzing COVID-19 Data using ANOVA Test," in *6th International Conference on Interactive Digital Media, ICIDM 2020*, pp. 1-6, 2020, https://doi.org/10.1109/ICIDM51048.2020.9339676.

BIOGRAPHY OF AUTHORS

Hero Wintolo earned his Bachelor of Electrical Engineering in 1997 and a Master of Computer science degree in 2003 from Universitas Gadjah Mada. He is currently serving as a full-time lecturer in Informatics at the Institut Teknologi Dirgantara Adisutjipto Yogyakarta. Hero is a member of the aerospace network and security research group, the aerospace avionics system research group, and the aerospace health informatics research group. Email: herowintolo@itda.ac.id. Orcid : https://orcid.org/0000-0002-4338-3238.

Yuliani Indrianingsih earned his Bachelor of Chemical Engineering in 1994 and a Master of Computer science degree in 2003 from Universitas Gadjah Mada. He is currently serving as a full-time lecturer in Informatics at the Institut Teknologi Dirgantara Adisutjipto Yogyakarta. Yuli is a member of the Aerospace Intelligent Systems and Data Engineering research group. Email: yuliani@itda.ac.id. Orcid : https://orcid.org/0000-0003-4380-6090 .

Wahyu Hamdani, bachelor of Informatics from Institut Teknologi Dirgantara Adisutjipto, is a programmer in this research. Email: dhaniabahari@gmail.com.

Syafrudin Abdie, earned his Bachelor of Mathematics in 1983 and a Master of Computer Sains degree in 2003 from Universitas Gadjah Mada. He is currently serving as a full-time lecturer in Electrical Engineering at the Institut Teknologi Dirgantara Adisutjipto Yogyakarta. Abdie is a member of the aerospace avionics system research group. Email: syafrudinabdie@itda.ac.id. Orcid : https://orcid.org/0000-0002-7130-8876.