[1]

TYPE YOUR ARTICLE TITLE [TIMES NEW ROMAN 16]

First Author[1]
Second Author[2],
etc. (Times New Roman 12; 1 space)
[1]First author's affiliation (Institution/University/etc.)
[2]Second author's affiliation
(Institution/University/etc.)
*Author correspondence: correspondent email
(Times New Roman; 1 space)

***Abstract* (Times New Roman 12)**

Abstract: The contents of the abstract are written in Times New Roman 12 font (1 space). The abstract consists of: main problem, objectives, methods, if there is anything new, please write down what the differences are with previous research, results, conclusions and recommendations for further research. The abstract is written in one paragraph, without references, without abbreviations/acronyms, and without footnotes. Abstracts are written not in mathematical form, questions and conjectures. The abstract is not the result of copying and pasting sentences in the contents of the manuscript. The English abstract must be a maximum of 250 words.

Keywords: Consists of 3 to 5 words and/or groups of words. Written in alphabetical order. Between keywords are separated by a semicolon (;).

Article History:
Submission date: - revision date: - accepted date:

I. INTRODUCTION

The introductory content includes background, novelty/newness, and the main problem of the study/research. The contents of the introduction are written in Times New Roman 12 font (1 space) [1].

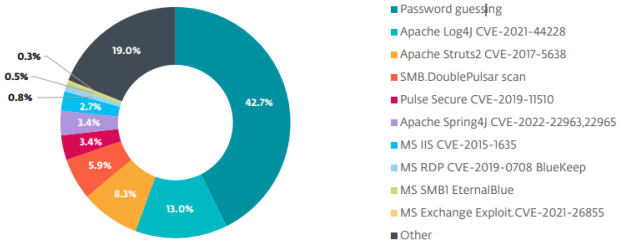


Fig 1. Source of external network intrusion [3]

II. LITERATURE REVIEW

The literature review includes scientific theories and concepts which are a reference source for writing studies/research as well as previous research. Reference/reading sources must be relevant to the topic being studied/researched, have the latest state of the art and reference year (last 10 years). Every reference source cited must be in the bibliography. The sub-title of the literature review is written in Times New Roman 12 font and the contents in Times New Roman 12 font (1 space) [2].

III. RESEARCH METHODOLOGY

This sub-chapter consists of: research design, data collection techniques and data testing (as needed). Methods reflect how to analyze studies/research to solve problems. From the analysis of this data, the results and discussion of the study/research are obtained. The contents of the method are written in Times New Roman 12 font (1 space).

Sub-heading of research methods (Times New Roman 12)

The research method sub-heading is written in Times New Roman 12 font and the contents in Times New Roman 12 font (1 space).

Table 1. List of test scenarios

Protocol	- HTTP - SSH - HTTPS

[1].

https://doi.org.....

	- FTP - IMAP - RDP
Interval	- 1 seconds - 10 seconds - 30 seconds
Actor	- 0 normal user, 1 threat actor - 3 normal user, 0 threat actor - 2 normal user, 2 threat actor - 3 normal user, 2 threat actor
Repetition	- Test #1 - Test #2 - Test #3

IV. RESULT AND DISCUSSION

Results and discussions are written in Times New Roman 12 font (1 space). Results should be separated from discussion. The results are not raw data, but rather data that has been processed/analyzed using certain methods. The discussion is the result of the interpretation of data analysis, if necessary linked to relevant scientific theories/concepts in the literature review. The results and discussion must answer the problem formulation and provide the impact of new knowledge. The contents of the results and discussion can be in the form of interpretations of discussion results, tables, pictures, diagrams, graphs, sketches, and so on.

Table and/or graph title (Times New Roman 10) and table contents Times New Roman 9 (1 space). Table titles are written above the table and arranged sequentially in one text, for example Table 1, Table 2, Table 3, and so on. If the table is quoted from another source, the source must be stated.

Picture arranged continuously, for example Figure 1, Figure 2, Figure 3, and so on. If the image is quoted/taken from another source, the source must be stated. These images include photos, diagrams, graphs, charts, sketches, prototypes, and databases.The page numbering is in the "CENTER" position starting with the number 1 and so on.

V. CONCLUSION

The contents of the conclusion are written in Times New Roman 12 font (1 space). The conclusion is an overview of the results of the discussion. The conclusion is written in one paragraph without any theory being quoted. Suggestions for further research are written in one paragraph in Times New Roman 12 font (1 space).

REFERENCES

The bibliography includes all reference source/readings cited in study/research. The reference/reading list is written systematically (alphabetical) in Times New Roman 12 font (1 space). The style for preparing the bibliography refers to the IEEE format. Writing quotations and bibliography is recommended using an automatic reference manager application Mendeley, Zotero, Endnote. Reference sources used as a bibliography include a minimum of 15 titles of scientific literature (minimum 80% primary reference sources and 20% secondary reference sources). Primary references consist of journals, proceedings/papers, research reports, theses, dissertations, while secondary references consist of general books and scientific information sources from the internet. Referenced library sources for the last 10 years.

Example :

[1] Bourgeois, David T.; Smith, James L.; Wang, Shouhong; and Mortati, Joseph, "Information Systems for Business and Beyond" (2019). Open Textbooks. 1.
[2] McAfee, A. & Brynjolfsson, “Investing in the IT that Makes a Competitive Difference”. Harvard Business Review. 86. 98-107 (2008).
[3] ESET Threat Report H1 2023, ESET Research,2023, https://www.welivesecurity.com/2023/07/11/eset-threat-report-h1-2023/. Accessed July, 12 2023.
[4] Goodgion, Jonathon S., "Active Response Using Host-Based Intrusion Detection System and Software-Defined Networking" (2017). Theses and Dissertations. 1575.
[5] Radhitya, Dimas. “Analisis implementasi Security Information and Event Management (SIEM) dengan berbasis wazuh pada sistem operasi Windows dan Linux” (2022). Fakultas Teknik Universitas Indonesia.

[6] Nova, F., Pratama, M. D., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. JITSI: Jurnal Ilmiah Teknologi Sistem Informasi, 3(1), 1-7.
[7] Pfau, Robert. The Security Lifecycle, SANS Institute, USA, 2003.
[8] N. Carr, "IT Doesn't Matter," Harvard Business Review, May 2003. [Online]. Available: https://hbr.org/2003/05/it-doesnt-matter. [Accessed: October 13, 2022].
[9] Center for Strategic & International Studies (CSIS), "Significant Cyber Incidents Since 2006," Center for Strategic & International Studies (CSIS), 2019.
[10] Check Point Software Technologies Ltd, "CYBER ATTACK TRENDS Check Point's 2022 Mid-Year Report," Check Point Software Technologies Ltd, 2022.
[11] Dr. Madhu Tyagi, "SECURITY AGAINST CYBER-CRIME: PREVENTION AND DETECT," Horizon Books (A Division of Ignited Minds Edutech P Ltd), 2017
[12] R. Stair and G. Reynolds, Principles of information systems. Cengage Learning, 2017.
[13] Committee on National Security Systems Instruction (CNSSI) No. 4009, "National Information Assurance Glossary," Committee on National Security Systems (CNSS), Apr. 2010.
[14] Microsoft, "What is SIEM?," Microsoft. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem. [Accessed: Jan. 5, 2023].
[15] Wazuh, "Components – Getting started," Wazuh. [Online]. Available: https://documentation.wazuh.com/current/getting-started/components/index.htm. [Accessed: Jan. 10, 2023].

https://doi.org.....