INTERNSHIP PRACTICE REPORT

FORENSICS OF CYBERSECURITY: TRAFFIC ANALYSIS EXERCISE - STEELCOFFEE TECHNOLOGICAL INSTITUTE OF THE PHILIPPINES (T.I.P)

By:

Rafa Nafisah
1900018087

DEPARTMENT OF INFORMATICS
FACULTY OF INDUSTRIAL TECHNOLOGY
UNIVERSITAS AHMAD DAHLAN
2023

APPROVAL

INTERNSHIP PRACTICE

FORENSICS OF CYBERSECURITY: TRAFFIC ANALYSIS EXERCISE - STEELCOFFEE

TECHNOLOGICAL INSTITUTE OF THE PHILIPPINES

Rafa Nafisah

1900018087

SUPERVISOR : Faisal Fajri Rahani S.Si., M.Cs. 27/01/2023 ...., ...
NIY : 60191224

EXAMINER : Nuril Anwar, S.T., M.Kom. 25/01/2023 ...., ...
NIY : 60160980

Yogyakarta, ...

Head of Informatics Department

01/02/2023

Dr. Murinto, S.Si., M.Kom.
NIY : 60040496

PREFACE

Praise and gratitude for the presence of Allah SWT, the Almighty God who has given His grace, guidance, and blessings so that the author can complete the report preparation, the author got a lot of help from various parties. Therefore, on this occasion, the author would like to express his gratitude to :

1. My Parents who have supported me in joining this program and also always pray for me to be a better human being.
2. Faisal Fajri Rahani S.Si., M.Cs. As a supervisor who has provided guidance to complete this exchange program.
3. Mr. Marte Nipas As a field supervisor has helped the author implement this project task.
4. Jesielle Miquiabas As a student buddy who helped collaborate in completing this project.

The author also realizes that in the implementation of this short course project and the preparation of this report, there are many shortcomings and errors. Therefore, the authors expect constructive criticism and suggestions, so that the next author's report can be better. Hopefully, this report can be useful for readers in general and for writers in particular.

Yogyakarta, 25 January 2023

Author,

Rafa Nafisah

TABLE OF CONTENTS

COVER i

APPROVAL ii

PREFACE iii

TABLE OF CONTENTS iv

IMAGE LIST v

TABLE LIST vi

ATTACHMENT LIST vii

CHAPTER I INTRODUCTION……………………………………………………………………………………..1

A. Background of Shortcourse 1

B. Shortcourse Identity 2

1. Shortcourse Category 2
2. Shortcourse Level *(National, International)* 2

CHAPTER II SHORTCOURSE OVERVIEW…………………………………………………………………..3

A. Shortcourse Organizer 3

B. Shortcourse Location 3

C. Shortcourse Execution Time 3

D. Shortcourse Scope 3

CHAPTER III SHORTCOURSE STAGES...4

A. Shortcourse Preparation Schedule 4

B. Shortcourse Activity Schedule 4

CHAPTER IV SHORTCOURSE INTERNSHIP PRACTICE RESULTS...6

A. Shortcourse Result 6

1. Shortcourse Process 6
2. Summary of Materials delivered during the Shortcourse 6

B. Products that were carried out during the Shortcourse 10

CHAPTER V CONCLUSION AND SUGGESTION……………………………………………………….17

A. Conclusion 17

B. Suggestion 17

ATTACHMENT..19

i. Brochure 19

ii. Certificate 19

iii. Log Book 19

iv. Documentation 21

IMAGE LIST

Figure 4.1 File HostandUser Wireshark 8

Figure 4.2 Applying Filters to pcap files 8

Figure 4.3 Follow TCP Stream File 8

Figure 4.4 File DNS 9

Figure 4.5 Domain Name System Description 10

Figure 4.6 Wireshark analysis 11

Figure 4.7 Find a Windows client and Username 12

Figure 4.8 Description of Windows client and Username 1 12

Figure 4.9 Description of Windows client and Username 2 13

Figure 4.10 Windows Infected Client 13

Figure 4.11 Filtering HTTP 14

Figure 4.12 Show HTTP object list window from Wireshark 14

Figure 4.13 Check SHA256 File hash 15

Figure 4.14 Check the Hash file on the Website 16

TABLE LIST

Table 3.1 Shortcourse Schedule 4

ATTACHMENT LIST

Attachment 1 SEAMEO TVET Brochure 19
Attachment 2 SEAMEO TVET Certificate 19
Attachment 3 Logbook Page 1 20
Attachment 4 Logbook Page 2 20
Attachment 5 Logbook Page 3 21
Attachment 6 Logbook Page 4 21
Attachment 7 Opening SEAMEO TVET 22
Attachment 8 Photo Session of Participants from UAD 22
Attachment 9 Forensics of Cybersecurity Conference 23
Attachment 10 Closing Ceremony of SEAMEO TVET 23