|  |  |  |
| --- | --- | --- |
| download logo**GROUP PROJECT**  **FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI**  **UNIVERSITI TEKNIKAL MALAYSIA MELAKA** | | |
| **PHYSICAL SECURITY & ELECTRONIC SURVEILLANCE** | | |
| **BITS 2423** | **SEMESTER 2** | **SESSION 2020/2021** |

**Group Project: Final Project BITS 2423**

**1.0 Learning Outcomes**

By the end of this course, the student will be able to:

1. Develop a partial design of the ESM architecture.
2. Integrate the ESM software you have downloaded in the previous laboratory exercise with ONE of the Agent.
3. Test the connectivity between the ESM and ONE of the Agent.
4. Collect log files and events from the partial ESM implementation.

**2.0 Instruction**

The heart of the Physical Security is the Enterprise Security Management (ESM). ESM provides a holistic approach to integrate guideline, policy and proactive measures. Thus, to implement the final project BITS 2423, these are the steps:

1. A complete ESM architecture shows the ESM Client, ESM Server and agent. The agent consists of IDS/IPS software tools, software-based firewall, any monitoring software tool and virtual private network (VPN). However, for this project, **a group of student need to partially design the ESM architecture**. Discuss among members to choose **ONLY ONE** of the agent to be included in the architecture.
2. Integrate the ESM software you have downloaded in the previous laboratory exercise with any IDS/IPS software tools **or** software-based firewall **or** any monitoring software tool **or** virtual private network (VPN).
3. Test the connectivity between the ESM and IDS/IPS software tools **or** software-based firewall **or** any monitoring software tool **or** virtual private network (VPN).
4. Collect the log files and events from the ESM tools that you have tested and monitored. Be creative to create scenarios in collecting various format of log files and events.

**RUBRIC OF REPORT SUBMISSION**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Marks** | **0-2** | **3-4** | **5-6** | **7-8** | **9-10** |
| Report  Organization | Report has no organization. | Report is poorly organized. | Report has no beginning, middle and ending section. | Report adequate with strong beginning, middle and ending. | Report well organized for example, Chapter 1,2,3,4 and 5, abstract, conclusion and references. |
| Content and Details | Content is not relevance  No information to explain about the matter. | Content is not informative and not accurate. Report has no supporting details. | Content is not relevance and less accurate. Report has few supporting details. | Content is informative and almost accurate. Report has adequate notes. | Content provides the gap of study and Report has supporting details of reference and interesting notes. |
| Writing Mechanics and Readability | High lack of writing skill and grammatical  error. Report is not complete. | Report is complete but has grammatical errors and lack of writing skill to show output. Report difficult to read. | Report is complete but has many errors in spelling, punctuation and grammar. | Report has several errors spelling, punctuation and grammar. Readable. | Report has no errors spelling, punctuation and grammar. Perfect. |
| Architecture Design | No architectural design | Lack of completion of the architectural design | Half complete architecture design | A complete and nice layout architecture design | A complete and informative architecture design |
| Connectivity and Testing | No connectivity | 20% connection is a success. | 50% success connection but 50% no connection. | 80% connection test is a success. | 100% connection test is a success. |
| Log File Analysis | No Log File | Few lines of Log File | Half of Log File obtained from the architecture setup. | More than half Log File received from the architecture setup. | Comprehensive Log File and easily to analyzed  by the security analyst. |
| Bonus –monitoring | No monitoring processes. | Lack of monitoring. | Some component can be monitored | Around 80% can monitoring | All connections able to monitor. |

COVER PAGE



**UNIVERSITI TEKNIKAL MALAYSIA MELAKA**

**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY**

**PROJECT OF BITS 2423**

**PHYSICAL SECURITY AND ELECTRONIC SURVEILLANCE**

**LECTURER: DR ZAHEERA ZAINAL ABIDIN**

**OVERALL MARKS – 10%**

**GROUP: 2 BITZ**

|  |  |  |
| --- | --- | --- |
| **BIL** | **NAME** | **MATRIC NUMBER** |
| 1. |  |  |
| 2. |  |  |
| 3. |  |  |
| 4. |  |  |
| 5. |  |  |
| 6. |  |  |