|  |  |
| --- | --- |
| **Server & Cloud Security**  Diploma in CSF/IT  Oct 2020 | Week 2 |
| Tutorial |
| **Server Security Controls & Principles** | |

1. Discuss the difference between policy, procedure, standard and guideline in your own words.

|  |
| --- |
| Policy are the foundation of the four words where it is to reflect on the objective of securing the program.  Standard is like action and rules use to direct user toward the policy.  Procedure is step or instruction to achieve the policy  And lastly, guideline is recommendation to user where the rule is more general compare to standard where the rules is specific |

1. Discuss how the below principles can help to improve a server’s security.

|  |  |
| --- | --- |
| **Fail Secure** | This prevent/reduce security vulnerabilities for attackers when a system fail or crash. For example, at the access controls systems, it should deny any request when they fail. |
| **Separation of duties** | This prevent a user from having too much power over a system by splitting responsibility among individual. This can also prevent spy from doing too much harm on an organization. |
| **Least Privilege** | It gives user the minimal level of access which is necessary to perform his work. Prevent an individual from able to access too much organization information and prevent hacker damage when they manage to get an individual account |
| **Compromise Recording** | It allows us to read how the system is performing. If compromise do happen, we have evidence and hits on what happen and how is happen.  We will be able to get error log too which can let us spot error that we do not spot often and fixed it as soon as possible. |

1. Discuss the challenges of managing logs.

|  |
| --- |
| 1. Keeping the confidentiality, integrity, and availability of generated logs from not being breached 2. Performing log analysis is hard and long; the log may not be able to group if the data in it is “good” or “bad”, so it will take time to analysis the data in the log which most of the time is millions on line be log. 3. Understand the log; Different system and software generate different logs which may show different message, which mean log manager may understand one log from this system but may not understand log from a different system. |

- The End -