Muhammad Izham Bin Norhamadi  
B032020039  
S2G1

# Mid Term Test: Part B

**a.**

1. OSSEC project provided by Atomicorp and OSSEC Foundation
2. Debian (Linux)

OSSEC is a mix of HIDS (host-based intrusion detection), log monitoring, and Security Information and Event Management (SIEM). Besides monitoring network for malicious activity and threats, OSSEC also check the integrity of the files in your systems and alert about them. Plus, OSSEC collects and analyses logs from operating systems, applications, and devices on the network to better understand the status of the network and notify changes such as application installed and a change of rule in the firewall. Lastly, active response allows OSSEC to take immediate action when specified alerts are triggered to prevent an incident from spreading before an administrator can take action.

1) OSSEC.NET, Getting started with OSSEC, <https://www.ossec.net/docs/docs/manual/non-technical-overview.html>

2) Wikipedia, OSSEC, <https://en.wikipedia.org/wiki/OSSEC>

**b.**

