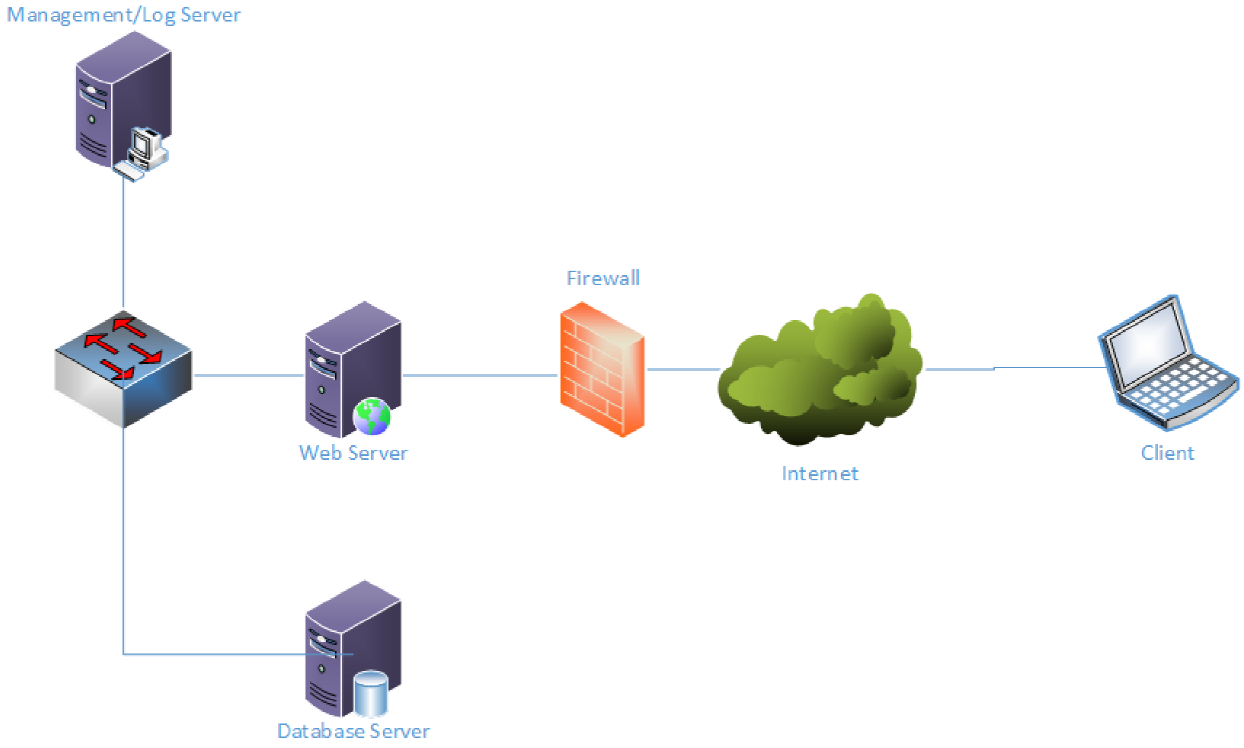
Homework Assignment #2 (100 points)

1. Address Space Layout Randomization is designed to make stack smashing attacks harder. Explain how Address Space Layout Randomization works (10 points). Describe an attack of how Address Space Layout Randomization can be circumvented (10 points)

2. Executable Stack Protection is another technology which can be used to protect against stack smashing attacks. Explain how ESP works (10 points). Provide an example of a class of attacks that can circumvent ESP (5 points). Describe how this class of attacks work (10 points)

3. You are tasked with hacking the President's Twitter Account. Develop an attack tree that details the various options and pathways to achieve that result (15 points)

4. Given the network diagram below – develop a threat model diagram and an attack surface analysis for this system detailing the following information (20 points):
    a. STRIDE elements for each component
    b. For the web server in particular, develop a "back-of-the-envelope" attack surface from both an internal network perspective as well as an external network perspective using the following information:
        i. open ports: 22, 111, 80, 443, 8080;
        ii. operating system: Ubuntu Server 16.0.4 with the following software installed
            1. SSHd (TCP/22)
            2. Postfix (TCP/25)
            3. Bind (TCP & UDP/53)
            4. Rpcbind (TCP/111)
            5. Apache (TCP/80, TCP/443)
            6. MySQL (TCP/3306)
            7. Tomcat (TCP/8080)
            8. Webmin (TCP/10000) – accessible from Management server only
        iii. The firewall provides external access to ports 22, 80, and 443
    c. Potential threats derived from the threat model (list at least 5 potential threats)



5. Define the various parts of the DREAD scoring system. What does each part of the DREAD scoring indicate? (5 points)

6. A threat has the following components of the overall DREAD score:
   a. Discoverability – 3
   b. Reproducibility – 3
   c. Damage Potential – 2
   d. Exploitability – 3
   e. Affected Users – 1

   Calculate the overall DREAD score. Describe the characteristics of each component (i.e. is it high, low, etc.). Is this threat a high, medium or low threat? (note: consider the overall scale of DREAD) (15 points)