**Security and Support in IT G (6689) – Assignment 2**

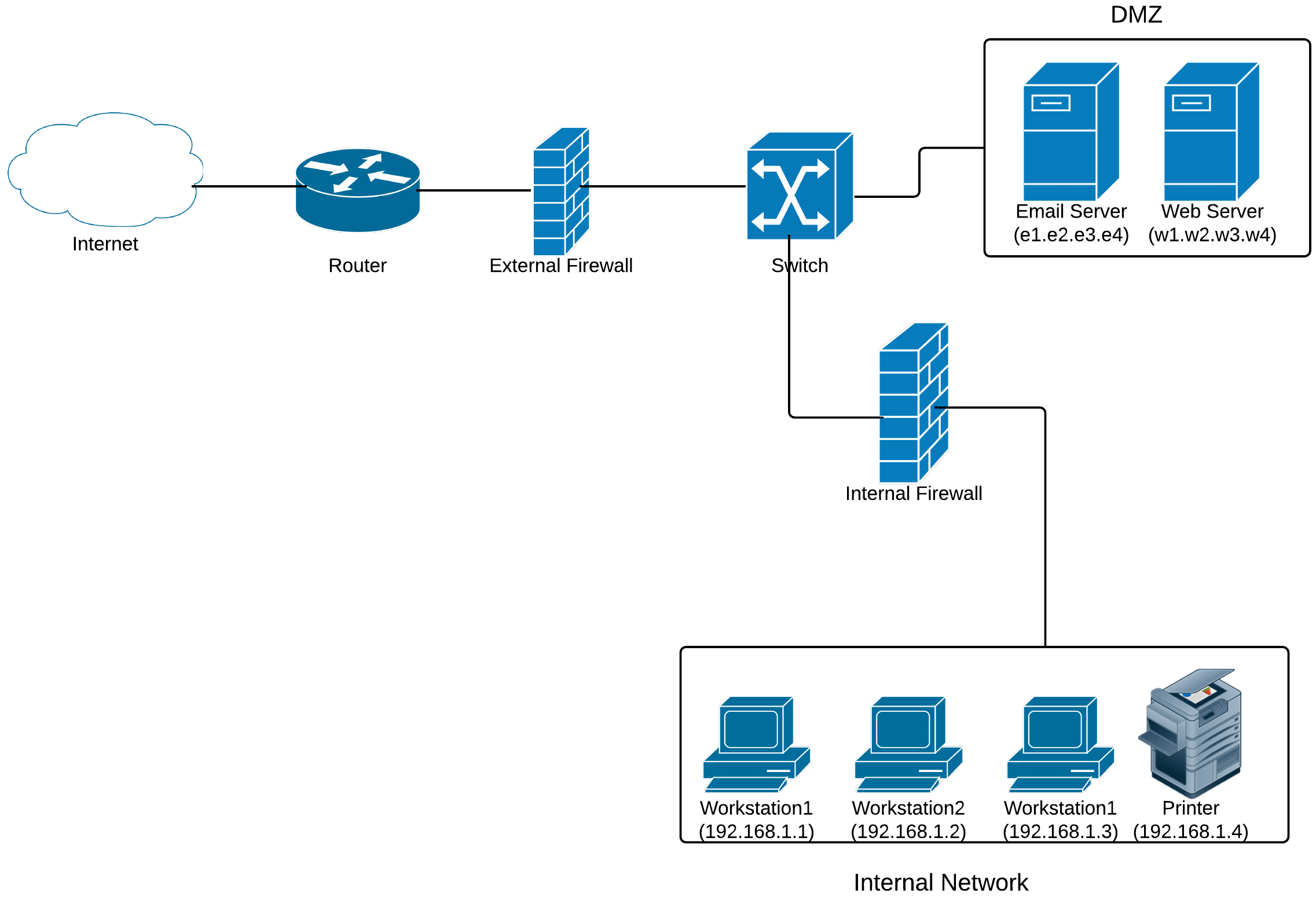
**Submitted by:**

**Name: Tenzin Dendup**

**Student ID: u3149399**

**Answers to Question 1**

Organization’s Network:



*Fig 1: Organization’s Network Diagram*

The organizations network is connected to the internet through their main router behind which sits the external firewall. A switch then divides the network into two, namely, the DMZ which has the webserver and the email server and the internal network.

The two servers (email and web) are provided with global IP address and are put in the DMZ since they need to allow connection from the internet. The workstations and printer are in the internal network and given private IP addresses under the same subnet. The internal network sits behind internal firewall which provides additional security. Hosts on internal network can access services on the internet and DMZ but are protected from the malicious connection requests and other threats from the internet. We also assume that the internal firewall acts as Network Address Translation (NAT) for internal network.

Firewall rules for External Firewall:

* Allow access to email server from the internet (SMTP & IMAP)
* Allow access to webserver from the internet (both http and https)
* Allow all outgoing connections from the organization’s network to the Internet (Assuming the global IP addresses of the organization is in the range **x1.x2.0.0/24**, which includes IP addresses of the servers)
* Allow Incoming traffic to ports great than 1024 since they are responses from external websites, email servers etc.
* Block any other connection request from outside

Chain INPUT (Policy ACCEPT)

target prot opt source destination

*ACCEPT tcp -- anywhere e1.e2.e3.e4 tcp:dpt:smtp state RELATED, ESTABLISHED*

*ACCEPT tcp -- anywhere e1.e2.e3.e4 tcp:dpt:imap state RELATED, ESTABLISHED*

*ACCEPT tcp -- anywhere w1.w2.w3.w4 tcp:dpt:https state RELATED, ESTABLISHED*

*ACCEPT tcp -- anywhere w1.w2.w3.w4 tcp:dpt:http state RELATED, ESTABLISHED*

*ACCEPT tcp -- anywhere x1.x2.0.0/24 tcp > 1024 state RELATED, ESTABLISHED*

*REJECT all -- anywhere anywhere reject-with-icmp-port-unreachable*

Chain OUTPUT (Policy ACCEPT)

*ACCEPT any -- x1.x2.0.0/24 anywhere any*

Firewall rules for Internal Firewall:

* Allow connection from DMZ servers to internal network workstations
* Allow access from internal network to all internet services
* Allow Incoming traffic to ports great than 1024 since they are responses from external websites, email servers etc.
* Block all connection request from internet to internal network

Chain INPUT (Policy ACCEPT)

target prot opt source destination

*ACCEPT tcp -- w1.w2.w3.w4 192.168.1.0/24 any*

*ACCEPT tcp -- e1.e2.e3.e4 192.168.1.0/24 any*

*ACCEPT tcp  -- anywhere 192.168.1.0/24  tcp>1024  state RELATED, ESTABLISHED*

*REJECT all -- anywhere 192.168.1.0/24 reject-with-icmp-port-unreachable*

Chain OUTPUT (Policy ACCEPT)

*ACCEPT any -- 192.168.0.0/24 anywhere any*

**Answer to Question 2**

Buffer Overflow

Buffer overflow is a condition that occurs in software programs where a large input is placed into a buffer or data holding area than the actual capacity allocated can accommodate, which results in overwriting other information in adjacent memory locations. This mainly happens due to use of unsafe function calls and careless programming. Attackers exploit buffer overflow vulnerabilities to crash a system or to insert especially crafted code, called shellcode, to gain control of the system. The consequences of buffer overflow problem are corruption of data, unexpected transfer of program execution to shellcode, memory access violations and program termination. If the program being affected is used to provide service to users, its termination may result is Denial of Service.

Programming techniques a software development team should adopt to avoid buffer overflow problems include:

* Choosing a modern high level programming language, like Java, that does not permit buffer overflow
* Making use of safe standard library functions
* Using safe coding standards like ensuring any code that writes to a buffer must check size of buffer for available space
* Including additional code that detects stack frame corruption
* Using Defensive and Secure Programming techniques like proper handling and interpretation of program inputs, correct algorithm implementation, ensuring that machine language corresponds to the algorithm being implemented, correct interpretation of data values etc.
* Correct and safe use of Environment variables, access privileges and temporary files

Nessus Report

The software development team of the organization can fix the problem by:

* Building a routine that checks web content for malicious code like malformed content, injection scripts and cross site scripts before it is executed by Firefox
* Adding code to do a thorough analysis of URLs so that the they do not load malicious scripts.
* Adding code to check externally linked contents like PDFs to ensure they are free of malicious code and scripts.

Accepting the recommendations given by the report, the organization should upgrade Firefox browser on all the desktop computers to the specified version which corrects all the issues listed in the report. The steps to be followed are:

1. Test the automated update on one test computer and ensure that the software is updated as required.
2. Then apply the automated update on some additional computers. Test and check that the updates on these computers are successful.
3. Once the test on some computers are successful, apply the automatic update on all the remaining computers.

A server is used to provide services to clients and is never used for common tasks like web browsing. To provide services, servers need to interact with computers from within and outside the organizations network which increases the chance of malicious attacks. In accordance with the principle of Hardening & Minimum Exposure, only required applications are installed on the server. Installing Firefox, which will never be used on the server, increases the probability of malicious attacks on the server using vulnerabilities found in Firefox. Also, once Firefox is installed on the server, its subsequent removal will result in its files and other data being left on the server which can be a source of vulnerabilities. The server can be attacked by malicious web contents and cross site scripts if Firefox is used to browse websites from the server. Therefore, due to it being an application that is not all required for the functioning of the server and also the risks associated with it, Firefox browser should not be installed on a server.

**References**:

1. Thomas A. Limoncelli, Christina J. Hogan and Strata R. Chalup, “*The Practice of System and Network Administration*” Second Edition, Addison-Wesley, 2007
2. William Stallings and Lawrie Brown, “*Computer Security: Principles and Practices*” third edition, Pearson Education Limited, 2015.