Coursework Part 1:

Title: Source Code Vulnerability

The following code listing is C program which takes a file name on the command line and then reads the file into a buffer. There are potentially exploitable buffer/variable overflow vulnerabilities in this program. Your task is to:

1. Find the buffer/variable overflows within the code
2. Explain how to change the code in order to avoid the vulnerabilities.
3. Explain how the vulnerabilities could be exploited in this particular case with detailed description of each step of the progression of the vulnerability.

```
#include <stdio.h>
#include <string.h>
#include <limits.h>

int main(int argc, char *argv[]) {

   FILE *fp;
   char filename[128];
   char strings[USHRT_MAX][80];
   unsigned short cnt = 0;

   strcpy(filename, argv[1]);

   fp = fopen (filename, "r");
   if (fp == NULL) {
        perror("Unable to open file: ");
        return(-1);
   }

   while (fscanf(fp, "%s", strings[cnt++] ) != EOF);

   fclose(fp);

   return(0);
}
```

Marking: This coursework part is worth 20% of your total G53SEC module mark. The breakdown of this mark is as follows:

- Correct identification of variable overflow vulnerabilities **(6 %)**
- Correct explanation of how the vulnerabilities can be avoided **(6 %)**
- Explanation of how the vulnerabilities can be exploited **(8 %)**

Coursework Part 2:

Title: Network Protection using a Firewall

Background: In today's information centric environment businesses and organisations cannot exist without a presence on the internet. Connectivity with customers as well as business partners is vital for the success of any business. In order to provide such internet presence, companies have to provide network based services such as web servers, email servers and many others. As internet presence and interconnectivity is increasingly becoming the major interface between businesses and their partners and customers, adversaries attempt to attack this interface for the purpose of extortion, espionage and data mining. Many techniques exist for the protection of various internet services. One of the most traditional yet still very effective approaches for defending services is the application of a firewall between servers providing various services and outsiders. This coursework deals with the deployment and set-up of firewalls and their policies within a corporate network.

Overview: In this coursework you are provided with a list of network components that a company wants to integrate into an operational network. This network should provide an interface between the company and the internet. This interface should allow for a number of services that are accessible by customers and business partners from the internet.

Your task is to design the *network topology* based on the network components provided, incorporating knowledge about *security* needs and requirements of providing network based services. You have to decide about the structure of the network and the correct deployment of *firewalls* within the network. Once your topology is complete it is vital to provide a set of *rules* for each deployed firewall in order to securely direct the flow of information between various parts of the network.

Network Components:

- 1x Web Server
- 1x FTP Server
- 1x Oracle Database Server
- 1x Company network printer
- 1x Company file server
- 2x Company Intranet subnets (A and B)
- 1x Facebook webserver
- 1x Gmail server
- 1x Twitter server
- 1x Internet cloud (the rest of the internet)

Example Network Topology:
An example network topology appears in Figure 1. Please note that this example does not contain all the required network components.

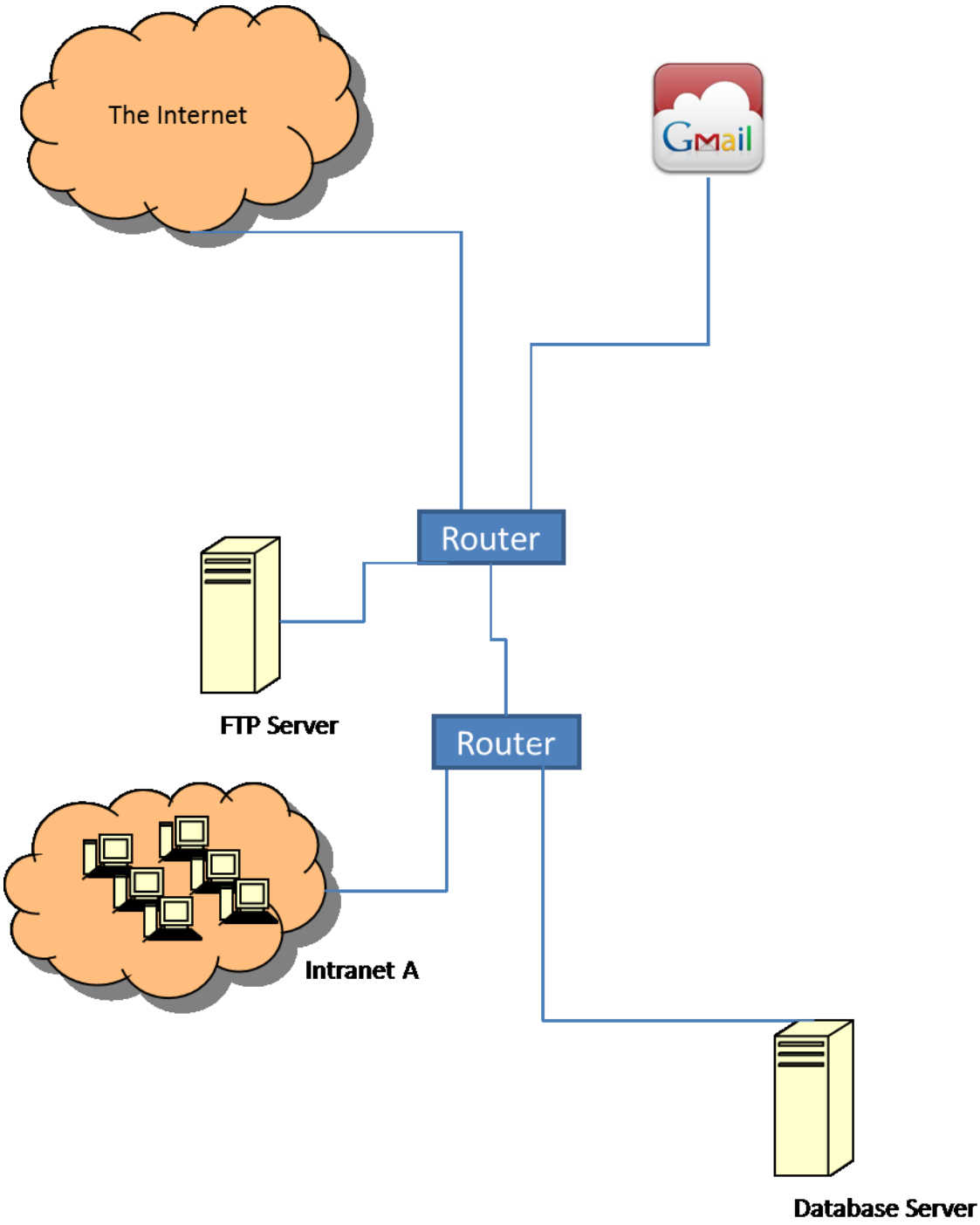

Figure 1 Example Topology

Topology Constraints:

- Everyone should have access to web pages served by the Web Server
- Access to the Web Service should be proxied via the Web Server only.
- Everyone on the internet should be able to access the FTP server using the FTP protocol. Intranet users should be able to access files using SSH secure copy.
- Any user from one of the intranet subnets should be able to use "Remote Desktop" to connect to a computer on the other subnet.
- Any user from intranet A should be able to access the File server using the SMB/CIFS protocol. Any user from intranet B should be able to access the file server using the NFS protocol.
- Any user from the intranets should be able to submit print jobs using *jetdirect* or *lpr* protocols.
- Users from intranet A should be able to access the Oracle database and web services running on the databases servers. Users from intranet B should only be able to ssh into the server for maintenance.
- The company users should be able to check their personal Google mail via the web/imap/pop but should not be able to use gmail to relay email.
- The company users should not be able to access facebook or twitter pages.
- Any user on the intranet subnets should be able to access the rest of the internet

Firewall Rule Grammar: In order to define a set of rules for each deployed firewall, it is important to use a grammar that captures necessary requirements of the network. Different firewall systems use different ways to write firewall rules. In this coursework you are required to use the following firewall rule structure:

Firewall Rules:

- ***Action***: Can be ALLOW or DENY
- ***Protocol***: Can be TCP or UDP
- ***Source Address, Destination Address***: Can be IP address, IP subnet, server name, or ANY

- ***Source Port, Destination Port***: Can be a number (3454), range of numbers (345-590), (1024-), or ANY

- **NOT**: Using "NOT" before a Protocol, Address or Port negates the matching. For example "ALLOW TCP from NOT evil.server.com ..." will pass traffic from every source that is not evil.server.com.

Rules precedence:
Rules are applied in the order they are listed, i.e. if rule No 3 allows certain traffic and rule No 4 denies it then the traffic will be **allowed**

Example:

Action	Protocol	Source	Destination	Src. Port	Dest. Port
Accept	*Tcp*	*Network X*	*Network Y*	*Any*	*22*
Deny	*udp*	*Host M*	*Host N*	*5500-7700*	*3128*

Make sure that you provide a set of rules for each deployed firewall!

References:
The bellow URL can be used as a reference for internet services names and port numbers:

http://www.iana.org/assignments/port-numbers

Marking: This coursework part is worth 20% of your total G53SEC module mark. The breakdown of this mark is as follows:

- Correct network topology **(5 %)**
- Correct deployment of firewalls **(5 %)**
- Correct specification of firewall rules **(5 %)**
- Short report specifying reasons behind selection of your network topology and firewall rules **(5 %)**