**Tutorial Sheet Week 4**

**Question 1**

Why is it good practice to rebuild a firewall before it is installed?

# Question 2

You are to do a Risk Analysis for the online banking system of a large national bank. What is the risk associated with the following events? Which would you devote most effort and funding to prevent? (Assume the bank is considering a network redesign.)

1. Phishing for customer accounts and PINs.
2. Transaction website hacked
3. Transaction database hacked
4. Denial of Service attack on transaction website

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Event A | Event B | Event C | Event D |
| Likelihood | 5 | 2 | 1 | 3 |
| Impact | 2 | 4 | 5 | 5 |
| Risk | 10 | 8 | 5 | 15 |

# Question 3

Suppose we have a stateful packet filter firewall that validates the three-way handshake in a TCP connection

1. What states will the firewall record for each step of the three-way handshake?
2. Write packet filtering rules for each state.

(For simplicity we do not consider direction or source address in answering this question).

Suggestion:

Construct a table that has the following columns:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| State | SYN set | ACK set | Action | New state |
| New | Yes | Yes | Deny |  |
| New | No | Yes | Deny |  |
| New | No | No | Deny |  |
| New | Yes | No | Allow | New Unreplied |

1