1. Now suppose a new worm break out. The feature of the worm is:

   1) It targets the TCP 8008 or UDP port 4004

   2) It contains the signature "03 0E FE CC A0" follow by "PASS : RECV" within the 20 bytes of the first one.

   3) The worm is coming from outside of our network (129.105.100.0/24).

Add a firewall rule to block that worm. Suppose the firewall use this kind of rule format:

Action	Src	port	dest	port	flags	comment
allow/block	IPsubnet, use * to refer any host	port number or * (refer any)	IPsubnet, use * to refer any host	port number or * (refer any)	flag can be TCP, UDP	The description of this rule

Write firewall rules based on the above format to the Ditty worm traffic towards our network (129.105.100.0/24).

Hint: assume that we do not have benign traffic on those services which the ditty worm rely on to propagate.

2. The purpose of this homework is develop skills in understanding the difference between a Security Policy, Standard, and Guideline. This exercise will focus on developing IT Security Policies.

Assignment:

Your assignment is to act as an outside consultant developing policies for a Fortune 100 company. The company business is food retailing with a global presence. You will be presented with a partially completed IT Security Policy that you are to complete. Please fill the missing policy statements in Section 2. Please just send me the missing part instead of the whole security policy file.

Note:

A hint for this exercise is that policies must be:

- General enough that standards can be developed from them.
- Specific enough for them to be targeted, practical, and useful.
- In plain English so that management, non-technical staff, and audit teams can understand and enforce them.

Network Configuration & Communication Policy

Document Number: XXXX-XXXX

Final Draft Version

Table of Contents