MSIT 458 Homework 7

Notes: 1. To be done by each group.
2. Please do not give a simple yes/no as results to some of the questions. Briefly explain why and how you obtain that result.

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. In this question, we explore some applications and limitations of a packet filtering firewall. For each of the question, briefly explain
1) can stateless firewall be configured to defend against the attack and how?
2) if not, what about stateful firewall ?
3) if neither can, what about application-level proxy?

a. Can the firewall prevent an online password dictionary attack from the external network on the telnet port of an internal machine?
b. Can the firewall prevent a user on the external network from opening a window on an X server in the internal network? Recall that by default an X server listens for connections on port 6000
c. Can the firewall block a virus embedded in an incoming email?
d. Can the firewall be used to block users on the internal network from browsing a specific external IP address?
e. Can the firewall prevent external users from exploiting a security bug in a

CGI script on an internal web server (the web server is serving requests from the Internet)?