1. The following diagram shows a network with a DMZ for its webserver. We want hosts inside the network and on the outside Internet to have access to the webserver, and we want hosts inside the network to have access to web servers on the Internet, but we don’t want hosts on the Internet to have access to any “internal” web servers, i.e. web servers that are in the internal network rather than the DMZ. Circle the annotations below for the traffic you want forwarded by each of the firewalls, and cross out the annotations for the traffic you want dropped by each of the firewalls.

![Diagram of network with DMZ and firewalls]

2. When a web server is installed on a host, the System Administrator (sysadmin) has a choice: the web server can run with the administrator account as its owner, or with a non-administrator account as its owner. Why is it safer not to have it run with the administrator account as its owner?

3. Suppose an organization you belong to has public pages and also has password-protected pages containing financial and personnel data for use by the people who work at the organization. Explain why splitting the pages up so that the public ones are housed on a web server in a DMZ, while the password-protected pages are kept on a web server on the internal network (see the diagram above), is more in keeping with the principle of defense in depth.

4. Why is it that keeping the software on your system up-to-date with the latest software versions and patches does not defend you against a “zero-day” exploit?
5) The lettered items below are categories of actions that might occur in a Computer Network Attack. The numbered items below are security measures you might take in Computer Network Defense.

Mark each numbered item with the letter of the attack action they help defend against. Note: In a few cases there might be multiple options, you need only provide one of them (preferably the most clear-cut).

Computer Network Attack Action Categories:

a. gaining remote access to a host on the target network
b. escalating privilege on one of the target hosts
c. using access on one host on the target network to then gain access to another host on the target network.
d. using privileged access to read secret information
e. infiltrating and concluding an attack without being noticed
f. flood packets onto a network to deny or degrade service

Computer Network Defense Measures: 4 Points each

___ 1. encrypt important files
___ 2. store password hashes rather than the passwords themselves
___ 3. enforce a policy of choosing strong passwords
___ 4. use different passwords for different accounts
___ 5. change the router's default admin password to one that is strong
___ 6. remove unneeded user accounts
___ 7. minimize the number of programs that run as root/administrator
___ 8. "sandbox" a server process
___ 9. keep webserver software up-to-date with the latest patches
___ 10. remove from your DNS server all programs that are not required to run and administer the DNS service.
___ 11. employ a firewall that blocks inbound traffic to services other than the few that must be publicly available (like http or DNS).
___ 12. employ a DMZ for a public-facing webserver
___ 13. regularly inspect logfiles (e.g. webserver access logs, login attempts, etc)
___ 14. monitor outbound network traffic for usual behavior (e.g. host X, which normally sends very little data out of the network, opens a TCP port 22 connection to some outside IP Address and sends gigabytes of data through it)
___ 15. set firewall rule to drop inbound packets based on rate from a source IP address