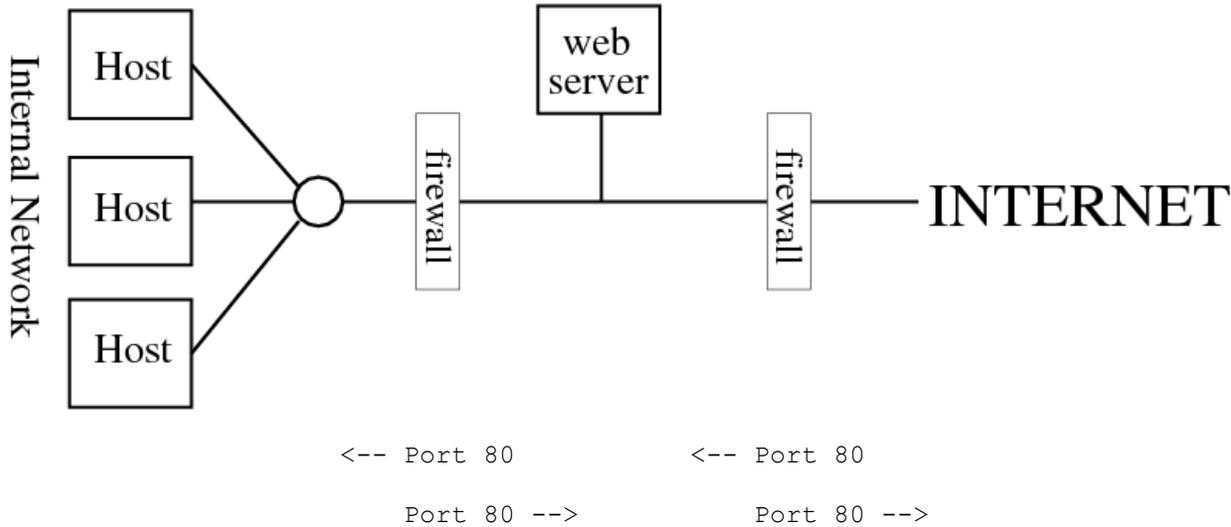


Hand in a stapled, printed copy with your answers.

**Homework: /SI110/Cyber Operations/Network Defense**

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.



2. When a webserver is installed on a host, the System Administrator (sysadmin) has a choice: the webserver 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. An important part of good cyber defense is vigilance. Good sysadmins should be regularly checking for signs of attack. If an attacker has exploited your webserver as part of some attack, where on the system might we find indications that the attack has occurred.

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?

Hand in a stapled, printed copy with your answers.

6) 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:

- \_\_\_ 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