Designing Security for a Microsoft Network

Name: ______________________________ Date: ______________

Network Security Quiz 1: Physical, Information, and Personnel Security

1. When there is a fire in the computer lab, what actions would we take (circle 3)
    a. Evacuate the room and push the fire alarm to evacuate the building
    b. If possible, unplug the unit that is smoldering, smoking or on fire
    c. Use a fire extinguisher and attempt to put out the fire
    d. Do nothing

2. What are some security checklist we use in our labs (circle 3)
    a. Physical
    b. Information
    c. Personnel
    d. Systematic

3. A web site designed to assist a computer security expert in identifying, categorizing, and neutralizing computer infestations.
    a. www.pandabears.com
    b. www.macabee.com
    c. www.gorton.com
    d. www.symantec.com

4. A government organizational assigned with providing businesses with national policy, list of threats, emergency procedures, and equipment lists for disasters.
    a. Internal Revenue Service (IRS)
    b. Occupational Safety Health Administration (OSHA)
    c. Federal Emergency Management Agency (FEMA)
    d. Operational Safety and Emergency Administration (OSEA)

5. You wish to set the default maximum password age for Windows 2003 to a reasonable time to secure your Windows 2003 network from document theft. Your network has been subjected to many authentication compromises in the last few months. How many days should pass before forcing a change in a user's password?
    a. 37 days
    b. 47 days
    c. 7 days
    d. 42 days

6. The customer is worried about information security and would like a raise the level of backup security for their network. You present the following plan to protect their data.
    a. You want to install a sprinkler system in the computer room.
    b. You add security lights in the parking lot with cages around the bulb to prevent breaking.
    c. You want to set up a backup system that replicates data. You select RAID level 1.
    d. Each employee is sent through a thorough background check.

7. Document such as letters, videos and web pages all have estimated worth for insurance and legal purposes.
    a. True b. False

8. Computer hardware and software inventories are (select 2 of the following)
   a. Submitted to the organization's insurance company as a written record of capital equipment
   b. Are collected annually in order to maintain an accurate list of what should be sold on Ebay
   c. Are kept updated monthly or quarterly and is part of the organization's DRP.
   d. Are submitted to the organization's management team to watch the Network Administrator

9. In conducting a security audit, check the following for paths to secure data (select 2)
   a. Data files written to the local hard drive
   b. Passwords written down and hidden near the workstation
   c. Company backup tapes in a brief case or purse
   d. Small cameras located in employee's coat

10. Attacking a high profile and secure government or corporate computer networks
    a. Only costs thousands of dollars in losses
    b. Does not matter since hackers attack military networks regularly
    c. Can be considered an act of war or terrorism
    d. Cannot be considered an act of aggression according to the UN

11. Network technicians and administrators want to be __________ to network attacks, using intelligence gathering techniques and ambushes.
    a. Progressive
    b. Proactive
    c. Reactive
    d. Resurgent

12. Every document is the Disaster Recovery Plan (DRP) requires (circle all that apply)
    a. Document control name
    b. Revision control
    c. Smart password protection
    d. Constant updating

13. A person is trying to gain access to a NASA server to get high definition images of the moon. What is their motivation in their cracking of the network? (circle all that are correct)
    a. Prestige or notoriety
    b. Maliciousness and desire to destroy
    c. Making a political statement
    d. Financial gain and theft
    e. Knowledge

14. After examining all the threats to our networks from Tornados to Snow Storms, we
    a. Write more reports and do nothing to prepare
    b. Collect all the necessary equipment from the Equipment needed section of the reports and store the items in strategic areas
    c. Go to meetings and just talk about impending doom
    d. Visit other companies to determine where we take their plan

15. More networks have been destroyed by
    a. Cracking
    b. Hacking
    c. Water or fire damage
    d. Incorrect amount of RAM

16. The term DRP stands for
    a. Disaster Removal Program
    b. Disaster Refuge Park
    c. Disaster Recoil Program
    d. Disaster Recovery Plan

17. Copies of the DRP should be located (circle 2)
    a. In the building so when there is a fire, the documents will be destroyed
    b. In Kansas, so we cannot get to it
    c. In our procession, so we can get to it in an emergency
    d. In the CEO procession, so he or she can get to it

18. The map of the United States shows that there is an abundant amount of nuclear reactors in the ____________, so we do not store our files in these areas.
    a. Central United States
    b. Midwest and East coast
    c. Northern Plains
    d. Region between the Rocky mountains and the Mississippi river

19. Profiling personnel in identifying a security threat can be a difficult task, but name a few signs of imminent danger. (select all that apply)
    a. Looking guilty
    b. Reporting false information on a regular basis
    c. Caught stealing small to medium sized software programs
    d. Unhappy employee, passed up for promotion after years of service
    e. Wears the wrong style of clothing

20. What is the minimum amount of teams within the incident response group?
    a. 1
    b. 2
    c. 3
    d. 4