Name: _____   Date: _____

Network Security Quiz 2: Physical, Information, and Personnel Security. Software attacks on networks.

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

2. What area of security are identification badges under
    a. Physical
    b. Informational
    c. Personnel
    d. Environmental

3. In computing, _____ is a criminal activity using social engineering techniques. They attempt to sensitive information by fraud, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.
    a. Wacking
    b. Phishing
    c. Hacking
    d. Exploring

4. Physical, personnel and information are
    a. The three types of network security that are audited at least once a month
    b. Are definitions of a domain container
    c. Are three types of inheritance
    d. Are definitions of a trust

5. The lowest suggested level of security control in a Windows 2003 network would be at Group level where access is controlled to the network and departmental files. The accounting department handles multiple accounts in excess of 1 billion dollars and institutes a color badge security system to enter their offices. This is an example of _____ security.
    a. Physical
    b. Environmental
    c. Personnel
    d. Informational

6. The disasters that the United States federal government states are most likely to occur in central Ohio are
    a. Hurricane, forest fire, earthquake, terrorist attack, tidal wave, mudslide and thunderstorms
    b. Tornado, hurricane, forest fire, earthquake, mudslide, terrorist attack, tsunamis, and nuclear
    c. Tornado, flood, terrorist attack, hazardous material spill, winter storm, nuclear, and thunderstorms
    d. Tornado, flood, earthquake, terrorist attack, hazardous material spill, Tsunami, mudslide and nuclear

7. Only _____ electrical cord coming into a computer, such as a telephone, coax or category 5e cable will allow a nearby lightning strike to enter the network. In the daisy chain, the voltage surge can destroy multiple machines before finding earth ground.
    a. 1   b. 2   c. 3   d. 4

8. The network administrator is using a Microsoft Management Console (MMC) to take inventory or the clients on their network. This is an example of _____ security.
    a. Physical
    b. Environmental
    c. Personnel
    d. Informational

9. 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 was stolen daily
    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 customers

10. 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)

11. The region between the Rocky mountains and the Mississippi river is the best place to
    a. Store corporate backups
    b. Have web servers
    c. Setup a shipping distribution center

12. A person who is proficient with computer programs and gains illegal access to a computer network or file
    a. Phreaker
    b. Cracker
    c. Wacker
    d. Attacker

13. 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

14. You, the Network Administrator will isolate the computer network from the larger network until the system is purged of a new worm, is the action you take when the worm is
    a. Defeating the security filters on the router
    b. Declared a level four threat on Symantec.com
    c. Declared a level fourteen threat at FEMA
    d. Already on all the machines in your company

15. Windows Critical Updates along with a firewall can be adequate defense against a worm (select 2)
    a. Since it takes over two months for a worm to spread on the Internet
    b. Since Critical Updates close the holes in the operating system used by worms
    c. Worms are released in the outer perimeter of the Internet to avoid detection
    d. Since firewalls have never been defeated by a worm

16. Network technicians and administrators want to be _____ to avoid network attacks, using intelligence gathering techniques and ambushes.

17. Every document in the _____ requires a document control name, revision control, password protection, and constant updating.

18. Sophisticated technique of authenticating one machine by forging packets from a trusted source is _____.

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

20. A _____ is a program designed to infiltrate through holes in operating systems and carry a payload that can damage a system, cause a nuisance or spread email messages.
    a. virus
    b. worm
    c. temporary file
    d. lash file

21. Network technicians and administrators can use _____ to probe files that are password protected.
    a. Hammers
    b. Scripts
    c. Viruses
    d. Worms

22. 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

23. VBScripts use _____ to enter data to the computer
    a. Blank keys
    b. Send keys
    c. Return keys
    d. Function keys

24. A dictionary attack to find a password can crack the password in
    a. A few months
    b. A few weeks
    c. A few days
    d. A few hours