Microsoft.Certdumps.98-367.v2014-11-27.by.Sherwin.218q

Number: 98-367
Passing Score: 800
Time Limit: 120 min
File Version: 16.5

http://www.gratisexam.com/

Exam Code:98-367

Exam Name:Security Fundamentals

Unit 1

QUESTION 1
Which of the following are valid risk responses? (Choose all that apply.) - (3)

A. Mitigation
B. Transfer
C. Investment
D. Avoidance

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following are considered removable devices or drives? (Choose all that apply.)- (3)

A. iPod
B. Netbook
C. USB flash drive
D. Floppy drive

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following would be considered appropriate security measures for a building's external security perimeter? (Choose all that apply.) - (2)

A. Motion detector
B. Parking lot lights
C. Turnstile

D. Security guards

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
You are traveling on business and are headed out to dinner with a client. You cannot take your laptop with you to the restaurant. What should you do with the device? (Choose the best answer.)

A. Lock the laptop in your car trunk.
B. Store the laptop out of sight in a dresser drawer.
C. Secure the laptop to a piece of furniture with a laptop security cable.
D. Check the laptop at the front desk.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
The process of eliminating a risk by choosing not to engage in an action or activity describes which of the following?

A. Mitigation
B. Residual risk
C. Avoidance

D. Acceptance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
You have just been promoted to Chief Security Officer for your auto parts manufacturing business and you are trying to identify technologies that will help ensure the confidentiality of your proprietary manufacturing techniques. Which of the following are technologies you could use to help with this endeavor? (Choose all that apply.) - (2)

A. Strong encryption
B. Security guards
C. Laptop safes
D. Strong authentication

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
The acronym CIA stands for which of the following?

A. Confidentiality, identity, access control
B. Confidentiality, integrity, access control
C. Confidentiality, integrity, availability
D. Control, identity, access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
You have been placed in charge of the corporate security department and your boss has asked you to help her understand what is meant by core security principles. Which of these explanations should you give to your boss?

A. Core security principles refer to the internal security perimeter when setting up a layered physical security environment.
B. Core security principles refer to the principles of confidentiality, availability, and integrity.
C. Core security principles refer to leveraging security best practices.
D. Core security principles refer to the four methods of addressing risk.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
As the Chief Security Officer for a small medical records processing company, you have just finished setting up the physical security for your new office. In particular, you have made sure that the parking lot is illuminated, that you have guards both at the door and performing periodic patrols, and that you have badge readers throughout the building at key locations. You also have put biometric access technology on the data center door. In addition, you have cameras in the parking lot, at building entrances, and at the data center entrances. This type of implementation is known as: (Choose the best answer.)

A. access control.
B. core security principles.
C. security best practices.
D. defense in depth.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
الدفاع فى العمق

QUESTION 10
What do you call the process of disabling unneeded services and ports to make a system more secure?

A. Reducing the surface attack area
B. Mitigating a Trojan horse
C. Security avoidance
D. Defense in depth

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
_____ is the characteristic of a resource that ensures that access is restricted to only permitted users, applications, or computer systems.

A. Confidentiality
B. integrity
C. availability
D. access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
If you are deploying technologies to restrict access to a resource, you are practicing the security principle known as _____

A. access control
B. defense in depth.
C. Mitigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Deploying multiple layers of security technology is called _____

A. access control
B. defense in depth.
C. Mitigation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
An action or occurrence that could result in the breach, outage, or corruption of a system by exploiting known or unknown vulnerabilities is a(n) _____

A. attack surface
B. threat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
You have just taken a new job as the Risk Manager for a medium-sized pharmaceutical company, and your first assignment is to perform a formal risk assessment. You will most likely record the results of your risk assessment in a(n) _____

A. risk register
B. residual risk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A secretary at your office just got off the phone with someone who said he was calling from the corporate IT department. The caller had a number of questions about the secretary's computer setup, and he asked for her user ID and password. In this situation, the secretary was most likely a victim of _____

A. social engineering.
B. attack surface
C. Mitigating a Trojan horse

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
The consistency, accuracy, and validity of data or information is called _____

A. integrity
B. Confidentiality
C. Avoidance
D. availability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
You are traveling for work and decide to use a computer in the hotel business center to check your email and pay several bills. When you sit down at the computer, you notice there is an extra connector between the keyboard and the computer. You have most likely encountered a(n) _____

A. keylogger

B. threat
C. social engineering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
You are the Risk Manager for a regional bank, and you have just deployed a new badge reader system to address an access control risk. Although your solution has mitigated the risk, there is still a small remaining risk associated with access control. This risk is known as the _____

A. residual risk
B. risk register
C. attack surface

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
المخاطر المتبقيه residual risk

QUESTION 20
The larger the _____ of a particular environment, the greater the risk of a successful attack.

A. attack surface
B. social engineering
C. defense in depth.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following terms indicates that information is to be read only by those people for whom it is intended?

A. confidentiality
B. integrity
C. availability
D. accounting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
What technology is not used to implement confidentiality?

A. encryption
B. access controls
C. auditing
D. authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

Which of the following makes sure that data is not changed when it not supposed to be?

A. confidentiality
B. integrity
C. availability
D. accounting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is not a response when dealing with a risk?

A. avoidance
B. mitigation
C. transfer
D. patching

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
What do you call the security discipline that requires that a user is given no more privilege necessary to perform his or her job?

A. principle of least privilege
B. risk transfer
C. reduction of attack surface
D. defense in depth

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
What do you call the scope that hacker can use to break into a system?

A. defense in depth
B. attack surface
C. principle of least privilege
D. risk mitigation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
What method used by a hacker relies on the trusting nature of the person being attacked?

A. social engineering
B. attack surface
C. principle of least privilege
D. risk avoidance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What is the best way to protect against social engineering?

A. stronger encryption
B. stronger authentication
C. employee awareness
D. risk mitigation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
What is needed to highly secure a system?

A. lots of time
B. more money
C. system update
D. disabled administrator account

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
What is the first line of defense when setting up a network?

A. physically secure the network
B. configure authentication
C. configure encryption
D. configure an ACL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which concept determines what resources users can access after they log on?

A. authentication
B. auditing
C. access control
D. defense in depth

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
What is used to provide protection when one line of defense is breached?

A. defense in depth
B. attack surface
C. principle of least privilege
D. risk mitigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
What is used to identify a person before giving access?

A. authentication
B. encryption

C. access control
D. auditing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What is used to verify that an administrator is not accessing data that he should not be accessing?

A. authentication
B. encryption
C. access control
D. auditing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What type of device can be easily lost or stolen or can be used for espionage?

A. processors
B. RAM chips
C. removable devices

D. servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
What is a physical or logical device used to capture keystrokes?

A. USB flash drive
B. PDA
C. Smartphone
D. keylogger

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
In dealing with risks, which response is done by buying insurance to protect your bottom line if such a disaster or threat is realized?

A. risk avoidance
B. risk acceptance
C. risk mitigation
D. risk transfer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
What processes and technologies will you use to keep these systems physically secure?

Case Study Title (Case Study):
You are the IT Manager for a 5,000-employee legal services company. You are in the process of rolling out new mobile devices to your sales department.

A. Docking stations: Virtually all laptop docking stations are equipped with security features. This may involve a key, a padlock, or both, depending on the vendor and model.
B. Laptop security cables: Used in conjunction with the USS (Universal Security Slot) these cables attach to a laptop and can be wrapped around a secure object like a piece of furniture.

   Laptop safes: These are steel safes specifically designed to hold a laptop and be secured to a wall or piece of furniture.
C. Theft recovery software: These applications enable the tracking of a stolen computer so it can be recovered.

   Laptop alarms: These are motion-sensitive alarms that sound in the event that a laptop is moved. Some are also designed in conjunction with a security cable system so that they sound whenever the cable is cut.
D. Keep your equipment with you: Mobile devices should be kept with you whenever possible. This means you should keep your mobile devices on your person or in your hand luggage when traveling. Similarly, keep your mobile devices in your sight when going through airport checkpoints.

   Use your trunk: If you are traveling by car and are unable to take your mobile device with you, lock it in the trunk when you park. Do not leave a mobile device in view in an unattended vehicle, even for a short period of time, and never leave it in a vehicle overnight.

   Use the safe: If you are staying in a hotel, lock your mobile device in a safe if one is available.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
which individuals used social engineering to break into a system, and list how they attempted to get access.

Case Study Title (Case Study):
You work for the Contoso Corporation. Your manager wants you to put together a training class about end-user security. To begin, use the Internet to research three cases or instances in

A. Answers will vary. But some of the common social engineering attack scenarios include the following:

A telephone or ISP repair person shows up to fix your telephone lines and asks for access to your wiring closet.

B. A person who poses as an auditor from the corporate office asks to set up in a conference room with a computer and network connection.

C. A person walks up to someone who works at the company and says that he left his keys or badge at home and he cannot get into a secure room. He asks if you can let him in.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
You are the Security Manager for a medium-sized bank. You have been asked to design a security solution to keep intruders out of the bank after hours. The three areas of the bank you need to secure are the parking lot, the building perimeter, and the vault

Case Study Title (Case Study):
List the technologies you would use in each of these areas.

A. Parking lot (external perimeter):
-Security cameras
-Parking lot lights
-Perimeter fence
-Gate with guard
-Gate with access badge reader
-Guard patrols

B. Building perimeter (internal perimeter):
-Locks (exterior doors, internal doors, office doors, desks, filing cabinets, etc.)
-Keypads
-Security cameras
-Badge readers (on doors and elevators)
-Guard desk
-Guard patrols
-Smoke detectors
-Turnstiles
-Mantraps

C. Vault (secure area):
-Badge readers
-Keypads

-Biometric technology (fingerprint scanner, retinal scanner, voice recognition)
-Security doors
-X-ray scanners
-Metal detector
-Cameras
-Intrusion detection systems (Light beam, infrared, microwave, and ultrasonic)

D. Nothing

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

Unit 2

QUESTION 1
Which of the following is not a method for authentication?

A. Something the user knows
B. Something the user owns or possesses
C. Encryption
D. Something the user is

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is not a biometric device?

A. Password reader
B. Retinal scanner
C. Fingerprint scanner
D. Face scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following services is used for centralized authentication, authorization, and accounting?

A. VPN
B. PGP

C. RADIUS
D. PKI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
What is the primary authentication method used on Microsoft Active Directory?

A. LDAP
B. Kerberos
C. NTLAN
D. SSO

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
The master time keeper and master for password changes in an Active Directory domain is:

A. PDC Emulator.
B. RID.
C. infrastructure master.
D. schema master.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Local user accounts are found in:

A. Active Directory.
B. Registry
C. SAM
D. LDAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A(n) _____ authorizes a user to perform certain actions on a computer.

A. permission
B. encryption algorithm
C. authentication protocol
D. right

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following file systems offers the best security?

A. FAT
B. FAT32
C. NTFS
D. EFS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which NTFS permission is needed to change attributes and permissions?

A. Full Control
B. Modify
C. Read and Execute
D. Write

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which type of permission is granted directly to a file or folder?

A. Explicit
B. Inherited
C. Effective
D. Share

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
If you copy a file or folder to a new volume, what permissions will that file or folder have?

A. The same permissions that it had before.
B. The same permissions as the target folder.
C. The same permissions as the source folder.
D. No permissions at all.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following uses an ACL?(choose 3)

A. NTFS folder
B. Active Directory user
C. Registry key
D. Login rights

Correct Answer: ABC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which type of key has one key for encryption and a different key for decryption?

A. Symmetric
B. Asymmetric
C. Hash function
D. PKI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which infrastructure is used to assign and validate digital certificates?

A. Asymmetric algorithm
B. Active Directory
C. PKI
D. VPN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which technology is used to encrypt an individual file on an NTFS volume?

A. BitLocker
B. BitLocker To Go
C. PPTP
D. EFS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A(n) _____ is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system.

A. personal identification number (PIN)
B. EFS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A pocket-sized card with embedded integrated circuits that is used for authentication is known as a(n) _____

A. smart card.
B. security token

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A device that may give you a second password to log in to a system is a(n) _____

A. smart card
B. security token.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
The _____ holds a copy of the centralized database used in Active Directory.

A. domain_controller
B. ownership

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
By default, your computer clock should not be off more than _____ minutes or you might have problems with Kerberos authentication.

A. five
B. Seven
C. Six

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 21
A(n) _____ defines the type of access over an object or the properties of an object such as an NTFS file or printer.

A. permission
B. ownership
C. auditing
D. registry

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
_____ permissions flow from a parent object to a child object.

A. personal identification number (PIN)
B. Inherited

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
When you cannot access a folder because someone removed the permissions so that no one can access it, you must take _____ of the folder.

A. ownership

B. Inherited
C. auditing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
The centralized database that holds most of the Windows configuration is known as the _____

A. auditing
B. permission
C. registry

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
To track a user's activities in Windows, you need to enable _____

A. registry
B. auditing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
What is the process of identifying an individual?

A. authentication
B. authorization
C. accounting
D. auditing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
What do you call the process in which a user is identified via a username and password?

A. authentication
B. authorization
C. accounting
D. auditing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What is the process of giving individual access to a system or resource?

A. authentication
B. authorization
C. accounting
D. auditing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
What is the process of keeping track of a user's activity?

A. authentication
B. authorization
C. accounting
D. authoring

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
What process prevents someone from denying that she accessed a resource?

A. accounting
B. authorization
C. sniffing
D. nonrepudiation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following is a secret numeric password used for authentication?

A. security token
B. digital certificate
C. digital signature
D. PIN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
What item, about the size of a credit card, allows access to a network and its resources?

A. digital certificate
B. smart card
C. security token
D. biometric

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
What type of authentication method identifies and recognizes people based on physical traits such as fingerprints?

A. digital certificates
B. WEP
C. biometrics

D. RADIUS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What authentication type is the default for Active Directory?

A. NTLM
B. Kerberos
C. MS-CHAP
D. MS-CHAPv2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What directory service is used with Windows domains?

A. Active Directory
B. E-Directory

C. PAM
D. Kerberos

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
What type of server runs Active Directory?

A. member server
B. file server
C. domain controller
D. NTLAN server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
When you access permissions to a folder, you should first grant permissions to _____ rather than users

A. groups
B. computers
C. collections
D. organizational units

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
When you create a local user on a computer running in Windows 7, where is the user account stored?

A. Active Directory
B. SAM
C. PAN
D. SQL database

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which type of group can be granted rights and permissions?

A. security
B. distribution
C. authorizing
D. SAM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
What type of electronic document contains a public key?

A. digital certificate
B. biometrics
C. PIN
D. PAN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
What authorizes a user to perform certain actions in Windows such as logging on or performing a backup?

A. permission
B. right
C. accessible
D. Key

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
When you grant access to print to a printer, what are you granting?

A. right
B. permission
C. accessible
D. key

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Where are users and permissions stored for an NTFS folder?

A. access log
B. access file
C. registry
D. ACL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
What type of permissions are assigned directly to a file or folder?

A. explicit
B. inherited
C. encompassing
D. overriding

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45

What is the process of converting data into a format that cannot be read by another user?

A. encryption
B. locking
C. keying
D. registering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which authentication sends the username and password in plain text?

A. MS-CHAP
B. CHAP
C. PAP
D. SPAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
In Windows, what do you use to enable auditing?

A. registry
B. group policies
C. NTFS permissions

D. access log

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
By default, the _____ group has full access to all resources within a domain?

A. Domain Admins
B. Domain User
C. Domain PowerUser

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
_____ allows you to log on once and access multiple related by different systems without having to log on again.

A. Single sign-on (SSO)
B. PowerUser

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
_____ is the term used to describe two or more authentication methods used to authenticate someone.

A. Multifactor authentication
B. Single sign-on (SSO)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
_____ is the standard for logging program messages for UNIX and Linux machines.

A. Syslog
B. authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
If you need to audit non-Microsoft products, you may need to use Syslog, standard for logging program messages that can be accessed by devices that would not otherwise would not have a method for communication. Cisco firewalls and routers, computers running Linux and UNIX, and many printers can use Syslog. It can be employed for computer system management and security auditing, as well as for generalized information, analysis, and debugging messages.

Unit 3

QUESTION 1
Which of the following are not valid password controls? (Choose all that apply.) 2

A. Minimum Password Age
B. Maximum Password Age
C. Maximum Password Length
D. Account Lockout Threshold
E. Password History

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following would be an acceptable password on a Windows 7 Professional system with Password Complexity enabled and Minimum Password Length set to eight? (Choose all that apply.) 3

A. Summer2010
B. $$Thx17
C. ^^RGood4U
D. Password
E. St@rTr3k

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
What is the maximum setting for Minimum Password Age?

A. 14
B. 999
C. 998
D. 256

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
You are setting up your first secure Windows 7 Professional workstation and you are setting the password history. What are the minimum and maximum settings you can use? (Choose the best answer.)

A. 0, 14
B. 1, 14
C. 0, 24
D. 1, 24
E. 0, 998

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following are common types of password attacks? (Choose Two answers)

A. Cracking
B. Man in the middle
C. Smurf
D. Spoofing
E. Brute force

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
One form of brute force password attack uses an extensive list of predefined passwords. What is this form of brute force attack called? (Choose the best answer.)

A. Bible attack
B. Cracking attack
C. Guessing attack
D. Dictionary attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
As the Chief Security Officer for a small medical records processing company, you suspect that a competitor will be attacking your network soon. Having worked in the business for a while, you're pretty sure that this competitor will try to run a dictionary attack against one of your Windows application servers. You want to be sure your competitor can't get into the server using this attack method. Which setting should you adjust in order to ensure this attack has a limited chance at success? (Choose the best answer.)

A. Minimum Password Length
B. Account Lockout Threshold
C. Password History
D. Maximum Password Age

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
You are the head of the corporate security department, and the Microsoft team has asked you for some assistance in setting the password controls on their new stand-alone server. Which Administrative Tool should you use to configure these settings?

A. Active Directory Users and Computers
B. Computer Management
C. Security Service
D. Local Security Policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9

What are the two new features introduced in Windows Server 2008 that permit the use of fine-grained password policies? (Choose all that apply.)2

A. Global Policy Object
B. Password Settings Container
C. Password Settings Object
D. Password Policy

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Why would you use a minimum password age?

A. To ensure that someone does not guess a password
B. To stop someone from trying over and over to guess a password
C. To make sure a user does not reset a password multiple times until he or she can reuse his or her original password
D. To automatically reset a password

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A set of rules that allows an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects, is known as a(n) _____

A. Global Policy Object (GPO).
B. Default Domain Policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
The number of incorrect logon attempts permitted before a system will lock an account is known as the

A. Reset account lockout counter after
B. Account Lockout Threshold.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
The setting that determines the number of unique passwords that must be used before a password can be re-used is the _____

A. Password History
B. Default Domain Policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
The type of attack that uses an extensive list of potential passwords is known as a(n) _____

A. dictionary attack.

B. service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
When you use special software to read data as it is broadcast on a network, you are _____ the network.

A. dictionary attack
B. sniffing
C.
D.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
The _____ needs to be less than or equal to the Account Lockout Duration

A. Reset account lockout counter after
B. Account Lockout Threshold
C.
D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
The highest setting that Account Lockout Duration can use is _____

A. 999
B. 1000
C. 998

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
In a Windows Server 2008 Active Directory, the _____ automatically applies in the event you have not set a fine-grained password policy.

A. Default Domain Policy
B. Global Policy Object (GPO).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
The three configuration settings for account lockout are _____, _____ and _____

A. Account lockout duration
B. Account lockout threshold
C. Reset account lockout counter after
D. Global Policy Object (GPO).
E. service

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A _____ account is one type of account you can configure so that the password does not expire.

A. service
B. Account Lockout Threshold

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
What is the most common form of authentication?

A. password
B. PIN
C. digital certificates
D. smart cards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Anytime you use a password, you should make it _____.

A. constantly changing
B. migrating
C. strong
D. simple

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What do you call a password that is at least seven characters long and uses three of the following categories (uppercase, lowercase, numbers, and special characters)?

A. healthy password
B. migrating password
C. standard password
D. complex password

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
What do you use to define how long a password is in Windows?

A. registry
B. Users applet in the Control Panel
C. group policies

D. NTFS files

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is not a complex password?

A. Platter*SAN
B. John!Taylor
C. Password01
D. ThereisTimetoLive&Die

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
What settings are used to keep track of incorrect logon attempts and lock the account if too many attempts are detected within a certain set time?

A. account lockout

B. password policy
C. authentication tracker
D. user parameters

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
What setting is used to prevent users from reusing the same password over and over?

A. minimum password age
B. maximum password age
C. password history
D. account lockout

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What prevents users from changing a password multiple times so that they can change it to their original password?

A. minimum password age
B. maximum password age
C. password history
D. account lockout

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 29
What setting forces users to change their password?

A. minimum password age
B. maximum password age
C. password history
D. account lockout

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
What type of attack tries to guess passwords by trying common words?

A. dictionary attack
B. brute-force attack
C. man-in-the-middle attack
D. smurf attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
What type of attack tries to guess passwords by every combination of characters?

A. dictionary attack
B. brute-force attack
C. man-in-the-middle attack
D. smurf attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
What malicious software captures every keystroke and sends it to a hacker?

A. dictionary software
B. password leaker
C. keylogger
D. sniffer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
What type of software can you use to view usernames and passwords broadcasted over the network?

A. dictionary software
B. password leaker
C. keylogger
D. sniffer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What is the generally accepted minimum password length?

A. 4
B. 6
C. 8
D. 12

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What are the only passwords that should not expire?

A. administrator accounts
B. power users
C. service accounts
D. standard user

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36

Which of the following should users not do when dealing with passwords?

A. Avoid allowing other users from seeing you type in your password.
B. Write down your password on a piece of paper and keep it near your computer.
C. Do not use names of children and pets.
D. Do not give your password to your co-workers
E. b, c, and d

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

Unit 4

QUESTION 1
Which of the following elements and issues should be considered when deciding whether to use a software or hardware firewall? (Choose all that apply.)3

A. Host operating system
B. Application conflicts
C. Operating system version
D. Firewall service efficiency
E. Stability

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following are layers of the OSI model? (Choose all that apply.)3

A. Physical
B. Control
C. Application
D. Network
E. Encryption

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

At which layer of the OSI model does routing occur?

A. Physical
B. Data link
C. Transport
D. Session
E. Network

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following are valid firewall types? (Choose the best answer.)2

A. Virtual
B. Network
C. Packet filtering
D. IPsec
E. Application

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following pieces of information are typically examined by a stateful inspection firewall?

A. IP address of the sending host

B. IP address of the receiving host
C. IP address of the router
D. Data packet type
E. Data packet size

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What is the purpose of NAP? (Choose the best answer.)

A. NAP translates private IP addresses to Internet-routable IP addresses.
B. NAP permits a firewall to perform deep inspection on packets.
C. NAP provides a mechanism to perform network analysis on captured packets.
D. NAP controls what systems are permitted to connect to a network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
An attack that relies on having a user execute a malicious script embedded in a web page is which kind of attack? (Choose the best

answer.)

A. Man in the middle
B. Brute force
C. Cross-site scripting
D. SQL injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
You have just purchased a new wireless access point for your small computer services company, and you want to ensure that only your systems are able to connect to the wireless network. To that end, you enable MAC address filtering and put the MAC addresses of all your computers in the permitted table. At what layer of the OSI model does this filtering occur?

A. Physical
B. Data link
C. Network
D. Transport
E. Session

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
You are the Information Security Officer for a medium-sized manufacturing company, and your sales team has just deployed a new e-commerce application to allow for the direct sale of your products to your customers. To secure this application, you are deploying an application firewall. At what layer of the OSI model does this filtering occur?

A. Physical
B. Data link
C. Network
D. Presentation
E. Application

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following are components of Network Access Protection? (Choose all that apply.)3

A. MAC address compliance
B. Health policy compliance
C. Limited access mode
D. IP address mode
E. Health state validation

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following are password-based attacks? (Choose all that apply.)2

A. Replay attacks
B. Network sniffer attacks

C. Brute force attacks
D. Man in the middle attacks
E. Dictionary attacks

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What type of attack relies on the attacker tricking the sending host into thinking his or her system is the receiving host, and the receiving host into thinking his or her system is the sending host? (Choose the best answer.)

A. Replay attack
B. Brute force attack
C. Man in the middle attack
D. Cross-site scripting attack
E. SQL injection attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following systems cannot participate in a NAP implementation? (Choose all that apply.) 2

A. Windows 7 Home
B. Windows 7 Home Premium
C. Windows XP Service Pack 2
D. Windows Vista Ultimate

E. Windows 7 Professional

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following are common uses for a VPN?2

A. Remote access
B. Server isolation
C. Intrusion detection
D. Extranet connections
E. Domain isolation

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following are common types of routing protocols? (Choose all that apply.)2

A. Link vector
B. Dynamic link
C. Distance link
D. Distance vector
E. Link state

Correct Answer: DE
Section: (none)

Explanation

Explanation/Reference:

QUESTION 16
You are a network administrator, and you have just been put in charge of registering your company's domain name and setting up the DNS so that people on the Internet can get to your website. Here,_____ can be used to ensure that your DNS entries are not poisoned by an attacker.

A. DNSSEC
B. IPSec

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
The two most common protocols you can use to create a VPN are _____ and _____

A. IPSec , SSL/TLS
B. DNSSEC ,DNS spoofing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
The three common types of protocol spoofing are _____,_____ and _____

A. ARP spoofing
B. DNS spoofing

C. IP address spoofing

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
The type of attack that relies on a weakness in an operating system or an application is known as a(n) _____

A. software vulnerability attack
B. DNS spoofing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
An attack that relies on access to a physical LAN segment is known as a(n) _____ attack

A. software vulnerability attack
B. network sniffing attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
An attack that records a stream of data, modifies it, and then resends it is known as a(n) _____ attack.

A. replay attack
B. DNS spoofing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
The two common types of Network Address Translation are _____ and _____

A. static
B. dynamic
C. DHCP

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
If you are setting up a WLAN in a corporate environment and you want to use 802.1x and a RADIUS server to secure the connections, you need to use _____ keys

A. WPA/WPA2
B. 802.1x enforcement
C. VPN
D. static

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
The four mechanisms used by NAP to restrict network access and enforce policies are _____ ,_____ , _____ and _____

A. IPsec enforcement
B. 802.1x enforcement
C. VPN enforcement
D. DHCP enforcement
E. WPA/WPA2

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A(n) _____ can be deployed to distract an attacker from the critical systems on your network.

A. network sniffing attack
B. honeypot
C. software vulnerability attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
What type of device isolates a network by filtering the packets that can enter it?

A. firewall
B. bridge
C. gateway
D. switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
What seven-layer model is often used to describe networking technologies and services?

A. OSI
B. TCP/IP
C. IPX/SPX
D. DIX

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
On which OSI layer do routers function?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
On which OSI layer do TCP and UDP function?

A. 1
B. 2
C. 3
D. 4

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
What OSI layer do switches and bridges use?

A. 1
B. 2
C. 3
D. 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
What port does SMTP use?

A. 21
B. 23
C. 25
D. 443

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
What port does LDAP use?

A. 25
B. 443
C. 389
D. 3389

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
What type of firewall filters packets based on IP address and ports?

A. packet-filtering
B. circuit-filtering
C. application-level
D. stateful

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What type of firewall is also known as a proxy server?

A. packet-filtering
B. circuit-filtering
C. application-level
D. stateful

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What type of firewall looks at the previous conversations to determine if a packet should enter a network?

A. packet-filtering
B. circuit-filtering
C. application-level
D. stateful

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Stateful inspection takes packet filtering to the next level. In addition to examining the header information of the packets traversing the firewall, a stateful inspection firewall considers other factors when determining whether traffic should be permitted across the firewall. Stateful inspection also determines whether a packet is part of an existing session, and that information can be used to decide whether

to permit or deny a packet

QUESTION 36
What Microsoft technology can verify that a client has the newest Windows updates and has an updated antivirus software package before being allowed access to the network?

A. IPSec
B. NAP
C. SCCM
D. SCOM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
What technology can you use to isolate a network of servers so that they cannot interact with other servers?

A. bridge
B. switch
C. router
D. VLAN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
What type of device looks at a packet and forwards it based on its destination IP address?

A. bridge
B. switch
C. router
D. VLAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which type of routing protocol sends the entire routing table to its neighbors?

A. distance vector
B. link state
C. scalable driven
D. infinity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which type of system detects unauthorized intruders and then takes action to stop them from proceeding?

A. IDS
B. IPS
C. VLAN
D. NAT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
What type of server would you install that would be used to trap a hacker?

A. honeypot
B. NAT
C. IPS
D. IDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
What special area serves as a buffer area between the Internet and the internal network and can be used to hold web servers that are accessed from the Internet?

A. DMZ
B. NAT
C. VLAN
D. PLC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
How many firewalls would you use to create a sandwich DMZ?

A. 1
B. 2
C. 3
D. 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
You have several Internet web servers that need to communicate with a SQL server. Where would you place the SQL server?

A. internal network
B. DMZ
C. Internet
D. isolated VLAN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following servers would you not place on the DMZ?

A. Internet web server
B. email relay servers
C. email mailbox servers
D. proxy servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
What technology allows a user at home to connect to the corporate network?

A. NAT
B. VPN
C. DMZ
D. PLC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which IPsec protocol provides integrity protection for packet headers, data, and user authentication but does not encrypt the data load?

A. AH
B. ESP

C. IKE
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Authentication Header (AH) provides integrity protection for packet headers, data, and user authentication. It can optionally provide replay protection and access protection. AH cannot encrypt any portion of packets. For AH to work with NAT, the IP protocol number 51 needs to be allowed across the firewall.

Unit 5

QUESTION 1
Which type of malware copies itself onto other computers without the owner's consent and will often delete or corrupt files?

A. Virus
B. Worm
C. Trojan horse
D. Spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which type of malware collects personal information or browsing history, often without the user's knowledge?

A. Virus
B. Worm
C. Trojan horse
D. Spyware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Your computer seems to be slow, and you notice that you have a different default web page than usual. What is most likely the cause of problems?

A. Your ISP has slowed your network connection
B. Your computer has been infected with malware.

C. You did not update your computer.
D. You accidentally clicked the turbo button.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Besides installing an antivirus software package, you should always _____ to protect your computer against malware.

A. keep your machine up to date with the latest security patches
B. reboot your computer on a regular basis
C. change your password on a regular basis
D. spoof your IP address

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A thoroughly tested, cumulative set of hotfixes and other patches is known as a(n):

A. recommended update
B. hotfix pack.
C. service pack.
D. critical update.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What technology is used by Windows to prevent unauthorized changes to your system?

A. UAC
B. Protected mode
C. Windows Defender
D. ProtectGuard

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
When using UAC, which of the following requires administrative permissions or rights?

A. Installing updates from Windows update
B. Changing the date and time
C. Resetting the network adapter
D. Installing drivers from Windows update or attached with the operating system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What mechanism is working when you try to change a computer's display settings and you get a pop-up asking whether you wish to continue?

A. Windows Firewall
B. Protected Mode
C. Windows Update
D. UAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
What host-based firewall software comes with current versions of Windows?

A. Windows Firewall
B. Windows Protected Mode
C. UAC
D. Windows GuardIt

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

What program would you use to configure IPsec on a computer running Windows Server 2008?

A. Windows Firewall with IPsec Plugin
B. IPsec Monitor
C. Windows with Advanced Security
D. IPsec Configuration console

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
If you have sensitive or confidential information stored in your offline files, it is recommended that you:

A. clear your cache.
B. encrypt the offline files.
C. clear your cookies.
D. execute ipconfig /renewip.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
You determine that legitimate emails are being blocked by your spam-blocking device. What should you do?

A. Flush out the quarantined items
B. Reboot the spam-blocking device
C. Add the address or domain for these emails to the white list
D. Add the address or domain for these emails to the black list

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
SMTP uses TCP port:

A. 43
B. 25
C. 80
D. 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
How many content zones are there in Internet Explorer?

A. 1
B. 2
C. 4
D. 8

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

Say that you receive an email stating that your account has just expired and asking you to log in to a legitimate-looking website to fix the problem. This is most likely an instance of:

A. phishing
B. pharming
C. phaking
D. IP address spoofing.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
_____ is software that is designed to infiltrate or infect a computer, usually with ill intent.

A. Malicious software (malware)
B. Windows Defender

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A(n) _____ is a self-replicating program that copies itself to other computers while consuming network resources.

A. worm
B. Virus
C. Trojan

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 18
Microsoft's antispyware program is called _____

A. Windows Defender
B. Malicious software (malware)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
For antivirus software to be effective, it must be kept _____

A. up to date
B. Before on 2 weeks ago

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
An example of a(n) **_____** is a message saying to delete the win.com file because it is a virus.

A. virus hoax
B. Worm

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 21
If you want to control what updates get pushed to clients within your organization, you would use _____ Or _____

A. Windows Update Server (WUS)
B. System Center Configuration Manager.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
_____ is when you are asked if you want to continue with an action and your desktop is dimmed and other programs are temporary halted until you approve the change.

A. Secure desktop
B. Windows Defender

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
_____ are copies of network files that are stored on your computer so that you can access them when you are not connected to the network.

A. Offline files
B. virus hoax

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
_____ is another name for junk email.

A. Spam
B. Offline files

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
_____ is an email validation system that is designed to verify that an email is coming from the proper email server.

A. Sender Policy Framework (SPF)
B. System Center Configuration Manager

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which type of malware can copy itself and infect a computer without the user's consent or knowledge?

A. virus

B. Trojan horse
C. rootkit
D. backdoor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
What type of self-replicating program copies itself to other computers on a network without any user intervention and consumes bandwidth and computer resources

A. virus
B. Trojan horse
C. worm
D. backdoor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What malware looks like a useful or desired executable program but is in reality program that is supposed to cause harm to your computer or steal information from your computer?

A. virus
B. Trojan horse
C. worm
D. backdoor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
What malware collects a user's personal information or details about your browsing habits without your knowledge?

A. virus
B. Trojan horse
C. worm
D. spyware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
What malware gives administrator-level control over a computer system?

A. rootkit
B. Trojan horse
C. worm
D. spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A rootkit is a software or hardware device designed to gain administrator-level control over a computer system without being detected. Rootkits can target the BIOS, hypervisor, boot loader, kernel, or (less commonly) libraries or applications.

QUESTION 31
What software component comes with Windows Vista and Windows 7 to defend against spyware?

A. Windows Firewall
B. Windows Defender
C. UAC
D. Windows Anti-virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
What do you call a message warning you to delete an essential Windows file?

A. virus hoax
B. keylogger
C. backdoor
D. worm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
What server can be used to install Windows updates for your organization?

A. SCOM
B. WSUS

C. IIS
D. WDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What do you call multiple Windows updates that have been packaged together as one installation and are well tested?

A. service packs
B. cumulative packs
C. critical update
D. optional update

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What Windows feature notifies you when something tries to make changes to your computer without your knowledge?

A. WDS
B. NAT
C. Windows Defender
D. UAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
What host firewall is included with Windows 7?

A. Windows Firewall
B. Windows Defender
C. Microsoft Protector
D. Microsoft Safety Net

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
What do you call unsolicited junk email?

A. spam
B. j-mail
C. junkettes
D. Infected mail

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
What email validation system is designed to stop spam that uses source address spoofing?

A. Foremost Relay System
B. Sender Policy Framework
C. Spam Checking Networking
D. Spoof Checker

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
What do spammers and hackers look for when they want to send email through your network?

A. open SMTP servers
B. open web servers
C. open POP3 servers
D. open FTP servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which tab in Internet Explorer settings would you use to delete history and cookies?

A. General
B. Privacy
C. Security
D. Advanced

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which Internet Explorer zone is the least secure?

A. Internet zone
B. local intranet zone
C. trusted sites zone
D. restricted sites zone

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
What technique is used to send you to a fake, but realistic-looking, website to verify your account information?

A. spoofing
B. smurfing
C. man-in-the-middle
D. phishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43

_____ is software that is designed to infiltrate or affect a computer system without the owner's informed consent.

A. Malware
B. Virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A _____ is a program that give someone remote, unauthorized control or a system or initiates an unauthorized task.

A. backdoor
B. Virus

Correct Answer:
Section: (none)
Explanation

Explanation/Reference: