NETWORK SECURITY

1. IS ONE OF THE MOST IMPORTANT ASSETS A COMPANY POSSESSES.

A) EMPLOYEES
B) RESOURCES
C) INFORMATION
D) MONEY

2. CONFIDENTIAL INFORMATION IS AVAILABLE TO EXTERNAL AUDIENCES ONLY FOR BUSINESS RELATED PURPOSES AND ONLY AFTER ENTERING A OR EQUIVALENT OBLIGATION OF CONFIDENTIALITY.

A) NONDEMOCRATIC AGREEMENT (NDA)
B) NONDISCLOSURE AGREEMENT (NDA)
C) NATIONAL DEMOCRATIC ALLIANCE (NDA)
D) NONDISCLOSURE ALLIANCE (NDA)

3. ORIGINALLY, THE ACADEMIC SECURITY MODEL WAS AND THE GOVERNMENT SECURITY MODEL WAS.

A) CLOSED AND LOCKED, WIDE OPEN
B) WIDE LOCKED, OPEN AND CLOSED
C) WIDE AND OPEN, WIDE AND CLOSED
D) WIDE OPEN, CLOSED AND LOCKED

4. AN APPROACH DOESN'T WORK WHEN YOU NEED TO ALLOW THOUSANDS OR MILLIONS OF PEOPLE TO HAVE ACCESS TO THE SERVICES ON YOUR NETWORK.

A) CLOSED-DOOR
B) OPEN-DOOR
C) WIDE-DOOR
D) LOCKED-DOOR

5. AN APPROACH DOESN'T WORK WHEN YOU NEED TO PROTECT THE PRIVACY OF EACH INDIVIDUAL WHO INTERACTS WITH THE SERVICES ON YOUR NETWORK.

A) CLOSED-DOOR
B) OPEN-DOOR
C) WIDE-DOOR
D) LOCKED-DOOR

6. AS MORE COMPANIES STARTED DOING BUSINESS ON THE INTERNET, CONCEPTS SUCH AS WERE DEVELOPED TO PROVIDE BUSINESS SERVICES OVER THE INTERNET.

A) SOFTWARE-AS-A-SERVICE (SAAS)
B) VIRTUAL(VPNS)
C) PERSONALLY, IDENTIFIABLE INFORMATION (PII)
D) STORAGE AS A SERVICE (SAAS) ANS: SOFTWARE-AS-A-SERVICE (SAAS)

7. WHAT CAN RESULT IN SERVICE OUTAGES DURING WHICH CUSTOMERS CANNOT MAKE PURCHASES AND THE COMPANY CANNOT TRANSACT BUSINESS?

A) VIRUS OUTBREAK

B) WEB SITE OUTAGE
C) DENIAL OF SERVICE (DOS) ATTACK
D) ALL OF THE ABOVE
E) NONE OF THE ABOVE

8. MEANS THAT SOFTWARE AND DATA CAN BE USED ON MULTIPLE PLATFORMS OR CAN BE TRANSFERRED/TRANSMITTED WITHIN AN ORGANIZATION, TO A CUSTOMER, OR TO A BUSINESS PARTNER.

A) PORTABILITY
B) ACCESSIBILITY
C) AUTHORITY
D) SHARING

9. IS CONCERNED WITH PROTECTING INFORMATION IN ALL ITS FORMS, WHETHER WRITTEN, SPOKEN, ELECTRONIC, GRAPHICAL, OR USING OTHER METHODS OF COMMUNICATION.

A) SOFTWARE SECURITY
B) INFORMATION SECURITY
C) NETWORK SECURITY
D) STORAGE SECURITY

10. IS CONCERNED WITH PROTECTING DATA, HARDWARE, AND SOFTWARE ON A COMPUTER NETWORK.

A) SOFTWARE SECURITY
B) INFORMATION SECURITY
C) NETWORK SECURITY
D) STORAGE SECURITY

11. THE THREE DS OF SECURITY STAND FOR:

A) DEFENSE, DEDICATION, AND DETERRENCE
B) DEFENSE, DETECTION, AND DISCIPLINE
C) DEFENSE, DETECTION, AND DETERRENCE
D) DEFENSE, DETECTION, AND DILIGENCE

12. WITHOUT ADEQUATE A SECURITY BREACH MAY GO UNNOTICED FOR HOURS, DAYS, OR EVEN FOREVER.

A) DETECTION
B) DETERRENCE
C) DEFENSE
D) ALL OF THE ABOVE

13. THE 3 ASPECTS OF SECURITY ARE:

A) DEFENSE, DEDICATION, AND DETERRENCE
B) DEFENSE, DETECTION, AND DISCIPLINE
C) DEFENSE, DETECTION, AND DETERRENCE
D) DEFENSE, DETECTION, AND DILIGENCE

14. PROVIDES A DEFENSIBLE APPROACH TO BUILDING THE PROGRAM.

A) SECURITY PROGRAM
B) SECURITY FRAMEWORK
C) PLANNING

D) SECURITY INITIATIVES

15. A SECURITY PROGRAM DEFINES THE PURPOSE, SCOPE, AND RESPONSIBILITIES OF THE SECURITY ORGANIZATION AND GIVES FORMAL AUTHORITY FOR THE PROGRAM.

A) CHARTER
B) MEMO
C) DOCUMENT
D) FILE

16. THE PROVIDES A FRAMEWORK FOR THE SECURITY EFFORT.

A) SECURITY PROGRAM
B) SECURITY FRAMEWORK
C) SECURITY POLICY
D) SECURITY INITIATIVES

17. CHANGE WITH EACH VERSION OF SOFTWARE AND HARDWARE, AS FEATURES ARE ADDED AND FUNCTIONALITY CHANGES, AND THEY ARE DIFFERENT FOR EACH MANUFACTURER.

A) STANDARDS
B) RULES
C) APPLICATION
D) FILES

18. GUIDELINES FOR THE USE OF SOFTWARE, COMPUTER SYSTEMS, AND NETWORKS SHOULD BE CLEARLY DOCUMENTED FOR THE SAKE OF THE PEOPLE WHO USE THESE TECHNOLOGIES.

A) STANDARDS
B) RULES
C) GUIDELINES
D) SECURITY

19. PROVIDES A PERSPECTIVE ON CURRENT RISKS TO THE ORGANIZATION'S ASSETS.

A) RISK ANALYSIS
B) PLANNING
C) GUIDELINES
D) SECURITY

20. COMPARES THE DESIRED STATE OF THE SECURITY PROGRAM WITH THE ACTUAL CURRENT STATE AND IDENTIFIES THE DIFFERENCES.

A) RISK ANALYSIS
B) SECURITY ANALYSIS
C) COMPARISON ANALYSIS
D) GAP ANALYSIS

21. IS A PLAN OF ACTION FOR HOW TO IMPLEMENT THE SECURITY REMEDIATION PLANS.

A) CHARTER
B) OUTLINE
C) ROADMAP
D) LAYOUT

22. THE DOCUMENTS HOW SECURITY TECHNOLOGIES ARE IMPLEMENTED, AT A RELATIVELY HIGH LEVEL.

A) CHARTER
B) SECURITY ARCHITECTURE
C) ROADMAP
D) LAYOUT

23. THE ACTIONS THAT SHOULD BE TAKEN WHEN A SECURITY EVENT OCCURS ARE DEFINED IN? THE INCIDENT RESPONSE PLAN.

A) CHARTER

B) SECURITY ARCHITECTURE

C) ROADMAP

D) INCIDENT RESPONSE PLAN

24. IS THE PROCESS OF DEFENSE, IS THE PROCESS OF INSURANCE, AND IS DECIDING THAT THE RISK DOES NOT REQUIRE ANY ACTION.

A) PLANNING, TRANSFERENCE, ACCEPTANCE
B) PLANNING, MITIGATION, ACCEPTANCE
C) TRANSFERENCE, MITIGATION, ACCEPTANCE
D) MITIGATION, TRANSFERENCE, ACCEPTANCE

25. IS A TERM USED TO DESCRIBE WHERE A THREAT ORIGINATES AND THE PATH IT TAKES TO REACH A TARGET.

A) THREAT VECTOR
B) ORIGIN VECTOR
C) TARGET VECTOR
D) TROJAN VECTOR

26. REFERS TO A TROJAN PROGRAM PLANTED BY AN UNSUSPECTING EMPLOYEE WHO RUNS A PROGRAM PROVIDED BY A TRUSTED FRIEND FROM A STORAGE DEVICE LIKE A DISK OR USB STICK, THAT PLANTS A BACK DOOR INSIDE THE NETWORK.

A) THREAT EXPLOIT
B) FRIEND EXPLOIT
C) GIRLFRIEND EXPLOIT
D) TRUSTED EXPLOIT

27. WHICH ARE THE GENERALLY RECOGNIZED VARIANTS OF MALICIOUS MOBILE CODE?

A) VIRUSES
B) WORMS
C) TROJANS
D) A AND B
E) A, B AND C

28. IS A SELF-REPLICATING PROGRAM THAT USES OTHER HOST FILES OR CODE TO REPLICATE.

A) VIRUS
B) WORM
C) TROJAN
D) NONE OF THE ABOVE

29. IF THE VIRUS EXECUTES, DOES ITS DAMAGE, AND TERMINATES UNTIL THE NEXT TIME IT IS EXECUTED, IT IS KNOWN AS?

A) TEMPORARY VIRUS
B) RESIDENT VIRUS
C) NONRESIDENT VIRUS
D) STEALTH VIRUS

30. IF THE VIRUS STAYS IN MEMORY AFTER IT IS EXECUTED, IT IS CALLED?

A) PERMANENT VIRUS
B) MEMORY-RESIDENT VIRUS
C) MEMORY NONRESIDENT VIRUS
D) NONE OF THE ABOVE

31. WHICH VIRUSES INSERT THEMSELVES AS PART OF THE OPERATING SYSTEM OR APPLICATION AND CAN MANIPULATE ANY FILE THAT IS EXECUTED, COPIED, MOVED, OR LISTED?

A) PERMANENT VIRUSES
B) MEMORY-RESIDENT VIRUSES
C) MEMORY NONRESIDENT VIRUSES
D) NONE OF THE ABOVE

32. IF THE VIRUS OVERWRITES THE HOST CODE WITH ITS OWN CODE, EFFECTIVELY DESTROYING MUCH OF THE ORIGINAL CONTENTS, IT IS CALLED?

A) OVERWRITING VIRUS
B) STEALTH VIRUS
C) NONRESIDENT VIRUS
D) PARASITIC VIRUS

33. IF THE VIRUS INSERTS ITSELF INTO THE HOST CODE, MOVING THE ORIGINAL CODE AROUND SO THE HOST PROGRAMMING STILL REMAINS AND IS EXECUTED AFTER THE VIRUS CODE, THE VIRUS IS CALLED?

A) OVERWRITING VIRUS
B) STEALTH VIRUS
C) PREPENDING VIRUS
D) PARASITIC VIRUS

34. VIRUSES THAT COPY THEMSELVES TO THE BEGINNING OF THE FILE ARE CALLED? PREPENDING VIRUSES

A) OVERWRITING VIRUS
B) APPENDING VIRUS
C) PREPENDING VIRUS
D) PARASITIC VIRUS

35. VIRUSES PLACING THEMSELVES AT THE END OF A FILE ARE CALLED?

A) OVERWRITING VIRUS
B) APPENDING VIRUS
C) PREPENDING VIRUS
D) PARASITIC VIRUS

36. VIRUSES APPEARING IN THE MIDDLE OF A HOST FILE ARE LABELED? MID-INFECTING VIRUSES.

A) MID-INFECTING VIRUSES
B) APPENDING VIRUSES
C) PREPENDING VIRUSES

D) PARASITIC VIRUSES

37. WHO WORKS BY POSING AS LEGITIMATE PROGRAMS THAT ARE ACTIVATED BY AN UNSUSPECTING USER?

A) VIRUS
B) WORM
C) TROJAN
D) NONE OF THE ABOVE

38. WHICH TYPE OF TROJANS INFECT A HOST AND WAIT FOR THEIR ORIGINATING ATTACKER'S COMMANDS TELLING THEM TO ATTACK OTHER HOSTS.

A) DIRECTED ACTION TROJANS
B) ZOMBIE TROJANS
C) REMOTE ACCESS TROJANS
D) NONE OF THE ABOVE

39. CIA STANDS FOR?

A) CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY
B) CONFIDENTIALITY, INTEGRITY, AND ACCESSIBILITY
C) CONFORMITY, INTEGRITY, AND ACCESSIBILITY
D) CONFIDENTIALITY, INTEGRITY, AND AUTHORITY

40. REFERS TO THE RESTRICTION OF ACCESS TO DATA ONLY TO THOSE WHO ARE AUTHORIZED TO USE IT.

A) CONFIDENTIALITY
B) AUTHORITY
C) ACCESSIBILITY
D) NONE OF THE ABOVE

41. ONION MODEL IS ALSO KNOWN AS:

A) PERIMETER SECURITY
B) DEFENSE IN DEPTH
C) BOTH OF THE ABOVE
D) NONE OF THE ABOVE

UNIT 03

1. WHICH MECHANISM IS USED FOR SECURING ACCESS TO A GIVEN SYSTEM BASED ON ONE CATEGORY OF IDENTIFICATION?

A) MULTI FACTOR AUTHENTICATION
B) TWO FACTOR AUTHENTICATIONS
C) SINGLE FACTOR AUTHENTICATION
D) NONE OF THE ABOVE

2. SYMMETRIC KEY CRYPTOGRAPHY IS USED FOR _____.

A) ENCRYPTION
B) DECRYPTION
C) ENCRYPTION AND DECRYPTION
D) NONE OF THE ABOVE

3.WHAT ARE THE MODES OF BLOCK CIPHERS?

A) OUTPUT FEEDBACK
B) ELECTRONIC CODEBOOK
C) CIPHER FEEDBACK
D) A AND C
E) ALL OF THE ABOVE

4._____ KEY IS USED FOR DECRYPTING THE DATA IN PUBLIC KEY CRYPTOGRAPHY.

A) PUBLIC
B) SYMMETRIC
C) PRIVATE
D) AUTHORIZATION

5._____ IS A SYSTEM FOR STORING AND MAINTAINING ENCRYPTION KEYS.

A) DIGITAL CERTIFICATE
B) PUBLIC KEY INFRASTRUCTURE
C) CERTIFICATE AUTHORITY
D) REGISTRATION AUTHORITY

6._____ ARE USED TO PROVIDE CERTIFICATE TO USERS, COMPUTERS AND OTHER SERVICES.

A) INTERMEDIATE CA
B) ROOT CA
C) DIGITAL CERTIFICATE
D) ISSUING CA

7. THE NEWEST FORM OF PORTABLE STORAGE IS THE _____.

A) PORTABLE HARD DRIVE
B) SOLID STATE DRIVE (SSD)
C) FLASH DRIVE
D) USB

8. _____ CAN BE ACCESSED BY MOST COMPUTERS AND OTHER DEVICES ON THE NETWORK

A) NETWORK-ATTACHED STORAGE (NAS)
B) STORAGE AREA NETWORKS (SANS)
C) HARD DRIVE
D) SERVER

9. A _____ IS THE MECHANISM AN ARRAY USES TO PRESENT ITS STORAGE TO A HOST OPERATING SYSTEM

A) VIRTUAL LANS (VLAN'S)
B) LOGICAL UNIT NUMBER (LUN)
C) ZONING
D) NONE OF THE ABOVE
E) SOLID STATE DRIVE (SSD)

10. _____ ARE ASSOCIATED WITH VULNERABILITIES AND THREATS PERTAINING TO THE PRIVACY AND CONTROL OF INFORMATION.

A) FORWARDING
B) AVAILABILITY RISKS
C) CONFIDENTIALITY RISKS
D) NONE OF THE ABOVE

11.A _____ IS AN ATTEMPT TO MAKE A COMPUTER RESOURCE UNAVAILABLE TO ITS INTENDED USERS

A) DATA TAMPERING
B) ACCIDENTAL MODIFICATION
C) DATA DELETION
D) DENIAL OF SERVICE (DOS) ATTACK

12. _____ STATEMENT RETRIEVES INFORMATION FROM DATABASE.

A) INSERT
B) SELECT
C) DELETE
D) UPDATE

13._____ REMOVES ANY CURRENT PERMISSIONS SETTINGS FOR THE SPECIFIED USERS OR ROLES.

A) DENY
B) GRANT
C) REVOKE
D) DELETE

14. _____ ARE DESIGNED TO AUTOMATICALLY BE "FIRED" WHENEVER SPECIFICATION ACTIONS TAKE PLACE WITHIN A DATABASE.

A) TRIGGERS
B) STORED PROCEDURES
C) VIEWS
D) NONE OF THE ABOVE

15.WHAT ARE THE FACTORS THAT CAN AFFECT THE IMPLEMENTATION OF BACKUP PROCESSES?

A) STORAGE SPACE
B) PROCESSING TIME
C) NETWORK BANDWIDTH
D) A AND B
E) ALL OF THE ABOVE

16._____ BACKUP CONSISTS OF COPYING ALL OF THE DATA THAT HAS CHANGED SINCE THE LAST BACKUP.

A) DIFFERENTIAL BACKUPS
B) TRANSACTION LOG BACKUPS
C) FULL BACKUP
D) NONE OF THE ABOVE

17._____ IS THE PROCESS BY WHICH PEOPLE PROVE THEY ARE WHO THEY SAY THEY ARE

A) AUTHORIZATION
B) DECLARATION
C) AUTHENTICATION
D) AUTHORITY

18._____ IS A NETWORK AUTHENTICATION SYSTEM BASED ON THE USE OF TICKETS.

A) MSCHAP
B) KERBEROS
C) CENTRAL STORAGE

D) CHAP

19. CHAP STANDS FOR?

A) CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL

B) CHALLENGE HARDWARE AUTHENTICATION PROTOCOL

C) CIRCUIT HARDWARE AUTHENTICATION PROTOCOL

D) CIRCUIT HANDSHAKE AUTHENTICATION PROTOCOL

20.THE INFORMATION THAT GETS TRANSFORMED IN ENCRYPTION IS

_____. A) PLAIN TEXT

B) PARALLEL TEXT

C) ENCRYPTED TEXT

D) DECRYPTED TEXT

21._____ USE HARDWARE- OR SOFTWARE-BASED AUTHENTICATORS THAT GENERATE A RANDOM SEED BASED ON THE CURRENT TIME OF DAY

A) SEQUENTIAL KEYS
B) CLOCK KEYS
C) TIME-BASED KEYS
D) NONE OF THE ABOVE

22._____ IS A CERTIFICATE-BASED SYSTEM THAT IS USED TO PROVIDE AUTHENTICATION OF SECURE WEB SERVERS AND CLIENTS AND TO SHARE ENCRYPTION KEYS BETWEEN SERVERS AND CLIENTS.

A) CERTIFICATE AUTHORITY
B) SECURE SOCKETS LAYER
C) DIGITAL CERTIFICATE
D) TRANSPORT LAYER SECURITY

23._____ ARE USED FOR A GRANULAR SELECTION OF PERMISSIONS.

A) READ
B) MODIFY
C) SPECIAL PERMISSION
D) MODIFY

24. AN ALGORITHM IN ENCRYPTION IS CALLED _____

A) ALGORITHM

B) PROCEDURE

C) CIPHER

D) MODULE

25. THE INFORMATION THAT GETS TRANSFORMED IN ENCRYPTION IS

_____ A) PLAIN TEXT

B) PARALLEL TEXT

C) ENCRYPTED TEXT

D) DECRYPTED TEXT

26. SP 800-63 IN NIST IS FOR _____.

A) RECOMMENDATION FOR BLOCK CIPHER MODES OF OPERATION: THE CMAC MODE FOR AUTHENTICATION
B) ELECTRONIC AUTHENTICATION GUIDELINE
C) FEDERAL AGENCY USE OF PUBLIC KEY TECHNOLOGY FOR DIGITAL SIGNATURES AND AUTHENTICATION
D) RECOMMENDATION FOR EAP METHODS USED IN WIRELESS NETWORK ACCESS AUTHENTICATION

27._____ KEY IS KEPT SECRET.

A) SYMMETRIC
B) PRIVATE
C) PUBLIC
D) SINGLE

28.PKI STANDS FOR _____.

A) PRIVATE KEY INFRASTRUCTURE
B) PUBLIC KEY INFRASTRUCTURE
C) PUBLIC KINETIC INFRASTRUCTURE
D) PROXY KEY INFRASTRUCTURE

29. WHICH OF THE FOLLOWING IS TRUE ABOUT PUBLIC KEY INFRASTRUCTURE?

A) PKI IS A COMBINATION OF DIGITAL CERTIFICATES, PUBLIC-KEY CRYPTOGRAPHY, AND CERTIFICATE AUTHORITIES THAT PROVIDE ENTERPRISE WIDE SECURITY.

B) PKI USES TWO-WAY SYMMETRIC KEY ENCRYPTION WITH DIGITAL CERTIFICATES, AND CERTIFICATE AUTHORITY.

C) PKI USES PRIVATE AND PUBLIC KEYS BUT DOES NOT USE DIGITAL CERTIFICATES.

D) PKI USES CHAP AUTHENTICATION.

30. WINDOWS SERVER 2008 R2 INTRODUCED VERSION ___ TEMPLATES, WHICH ADD SUPPORT FOR THE NEWER MICROSOFT CRYPTO-API, GIVING ADMINISTRATORS THE ABILITY TO PRODUCE CERTIFICATES USING THE MORE ADVANCED AND SECURE ELLIPTIC CURVE CRYPTOGRAPHY (ECC) CRYPTOGRAPHY SERVICE PROVIDERS (CSPS).

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

31.SPECIFIC CA ROLES ARE _____.

A) CA MANAGER
B) CA CONTROLLER
C) CA ADMINISTRATOR
D) ALL OF THE ABOVE
E) A AND C

32.STORAGE INFRASTRUCTURE CONSISTS OF _____.

A) STORAGE NETWORKS

B) ARRAYS
C) SERVERS
D) ALL OF THE ABOVE
E) B AND C

33. REPRODUCTION OF TRAFFIC AND DATA THAT WAS PREVIOUSLY SENT ON A NETWORK IS CALLED _____.

A) PACKET REPLAY
B) PACKET SNIFFING
C) ESPIONAGE
D) NONE OF THE ABOVE

34. FULL FORM OF OLTP IS _____.

A) ONLINE TRANSACTION PROCESSING
B) ONLINE TRANSACTION PROGRAM
C) ORACLE TRANSACTION PROCESSING
D) ONLINE TERMINAL PROCESSING

35. WHAT ARE THE RECOVERY REQUIREMENTS OF DATA?

A) COST OF DOWNTIME
B) VALUE OF THE DATA
C) AMOUNT OF ACCEPTABLE DATA LOSS
D) ALL OF THE ABOVE
E) NONE OF THE ABOVE

36. WHAT ARE THE TYPES OF BACKUPS?

A) FULL BACKUPS
B) HALF BACKUPS
C) TRANSACTION LOG BACKUPS
D) A AND B
E) ALL OF THE ABOVE

37. AN _____ IS ANY UNEXPECTED DOWNTIME OR UNREACHABILITY OF A COMPUTER SYSTEM OR NETWORK.

A) DOWNAGE
B) OUTAGE
C) BREAKDOWN
D) MODIFICATION
E) ALL OF THE ABOVE

38. TYPES OF RISKS TO DATABASE?

A) DATA LEAKAGE
B) FRAUD
C) INAPPROPRIATE ADMINISTRATOR ACCESS
D) A AND B
E) ALL OF THE ABOVE

39. FULL FORM OF NAS IS _____

A) NEW AREA STORAGE
B) NETWORK AROUND STORAGE

C) NETWORK AREA STORAGE
D) NEW AROUND STORAGE

40. A _____ ISSUES, CATALOGS, RENEWS, AND REVOKES CERTIFICATES UNDER THE MANAGEMENT OF A POLICY AND ADMINISTRATIVE CONTROL

A) CERTIFICATE AUTHORITY (CA)
B) DIGITAL CERTIFICATE
C) CA MANAGER
D) ROOT CA

41. WHAT CONTROL CAN BE USED TO HELP MITIGATE IDENTIFIED RISKS TO ACCEPTABLE LEVELS?

A. AUTHENTICATION B. AUTHORIZATION C. DECRYPTION D. MANAGEMENT 42. WHICH ONE IS THE

KEY NETWORK DESIGN STRATEGY?

A. PERFORMANCE B. COST OF SECURITY C. ROUTING D. ENCRYPTION

43. WHICH TECHNOLOGIES MAY BE CONSIDERED BY THE DESIGN TEAM TO PREVENT ONE APPLICATION FROM CONSUMING TOO MUCH OF BANDWIDTH?

A. ELECTRONIC SECURITY PERIMETER(ESP)
B. SOFTWARE-AS-A-SERVICE(SAAS)
C. PUBLIC SWITCHED TELEPHONE NETWORK(PSTN)
D. QUALITY OF SERVICE(QOS)

44. HOW MANY LAYERS DOES CISCO INTERNETWORKING MODEL HAS?

A. THREE B. FOUR C. TWO D. ONE

45. WHAT IS CORE LAYER'S PRIMARY FOCUS?

A. FILTERING B. ENCRYPTION C. PERFORMANCE D. COMPRESSING

46. _____ LAYER IS COMPOSED OF THE USER NETWORKING CONNECTIONS.

A. ACCESS LAYER B. CORE LAYER C. DISTRIBUTION LAYER D. FIREWALL

47. WHICH ARCHITECTURING APPROACH OFFERS HIGHER PERFORMANCE AND LOWER COST BUT ALSO BRINGS SPECIAL SECURITY CONSIDERATIONS INTO PLAY.

A. SINGLE-TIER B. THREE-TIER C. MULTI-TIER D. COLLAPSED TWO-TIER

48. WHAT HELPS US TO UNDERSTAND HOW TO USE ROUTERS AND SWITCHES TO INCREASE THE SECURITY OF THE NETWORK?

A. SECURITY NETWORK DESIGN
B. WIRELESS NETWORK SECURITY
C. NETWORK DEVICE SECURITY
D. FIREWALLS

49. THE DOMINANT INTERNETWORKING PROTOCOL IN USE TODAY IS KNOWN AS _____.
A. TCP/IP B. HTTPS C. FTP D. UTM

50. MAC ADDRESSES ARE ____ BIT HEXADECIMAL NUMBERS THAT ARE UNIQUELY ASSIGNED TO EACH HARDWARE NETWORK INTERFACE BY THE MANUFACTURER.

A. 8 B. 24 C. 48 D. 64

51. IPV4 ADDRESSES ARE ___ BITS.

A. 8 B. 32 C. 64 D. 128

52. IPV6 ADDRESSES ARE ___ BITS.

A. 128 B. 32 C. 24 D. 64

53. THE HOST USES THE _____, WHICH FUNCTIONS BY SENDING A BROADCAST MESSAGE TO THE NETWORK THAT BASICALLY SAYS, "WHO HAS 192.168.2.10, TELL 192.168.2.15".

A. NETWORK INTERFACE CARD(NIC)
B. DOMAIN NAME SERVER(DNS)
C. ADDRESS RESOLUTION PROTOCOL (ARP)
D. OPEN SYSTEM CONNECTION (OSI)

54. HOW MANY LAYERS DOES OSI MODEL CONTAIN?

A. FIVE B. SIX C. FOUR D. SEVEN

55. _____ AN OSI-MODEL LAYER IS USED TO CONVERT APPLICATION DATA INTO ACCEPTABLE AND COMPATIBLE FORMATS FOR TRANSMISSION. AT THIS LAYER, DATA IS ENCRYPTED AND ENCODED AND ENCRYPTED.

A. PRESENTATION B. APPLICATION C. TRANSPORT D. NETWORK

56. WHICH IS MOST WELL-KNOWN APPLICATION-LAYER PROTOCOLS IN USE TODAY?

A. TCP/IP B. UDP C. HTTP D. FTP

57. WHICH LAYER PROVIDES MECHANISM FOR TWO HOST TO MAINTAIN NETWORK CONNECTIONS.

A. DATA-LINK LAYER B. SESSION LAYER C. PHYSICAL LAYER D. TRANSPORT LAYER 58. WHICH

LAYER PROVIDES UNIQUE ADDRESS TO EVERY HOST ON THE NETWORK. A. APPLICATION LAYER B.

PHYSICAL LAYER C. TRANSPORT LAYER D. NETWORK LAYER

59. ____ LAYER IS COMPOSED OF TWO SUB LAYERS: MEDIA ACCESS CONTROL (MAC) AND LOGICAL LINK CONTROL (LLC).

A. DATA-LINK B. TRANSPORT C. APPLICATION D. PHYSICAL

60. AS THE SIZE OF THE NETWORK INCREASES, THE DISTANCE AND TIME A PACKET IS IN TRANSMIT OVER THE NETWORK ALSO _____, MAKING COLLISION MORE LIKELY.

A. INCREASES B. DECREASES C. ALL OF THE ABOVE D. NONE OF THE ABOVE 61.

ROUTERS AND SWITCHES OPERATE AT LAYERS ___ AND ___ RESPECTIVELY. A. TWO

AND THREE B. THREE AND TWO C. ONE AND TWO D. THREE AND FOUR. 62. IN WHICH

TWO WAYS ROUTERS LEARN THE LOCATIONS OF VARIOUS NETWORKS?

A. DYNAMICALLY AND STATICALLY
B. DYNAMICALLY AND MANUALLY
C. ALL OF THE ABOVE
D. NONE OF THE ABOVE

63. WHAT ARE THE TWO MAIN TYPES OF LAYER THREE (ROUTING) PROTOCOLS?

A. DYNAMIC AND STATIC
B. DISTANCE-VECTOR AND LINK-STATE
C. MANUAL AND STATIC

D. NONE OF THE ABOVE

64. WHICH ONE OF THE FOLLOWING IS A NETWORK HARDENING METHOD?

A. REMOTE ACCESS CONSIDERATIONS
B. NETWORK MODELLING
C. THE COST OF SECURITY
D. PATCHING

65. WHAT CAN BE CONFIGURED TO PERMIT OR DENY TCP, UDP, OR OTHER TYPES OF TRAFFIC BASED ON THE SOURCE OR THE DESTINATION ADDRESS.

A. DISABLING UNUSED SERVICES
B. ACCESS CONTROL LISTS
C. PATCHING
D. SWITCH SECURITY PRACTICES

66. WHICH ONE OF THE FOLLOWING COMES UNDER DISABLING UNUSED SERVICES?

A. ACCESS CONTROL LISTS
B. ADMINISTRATIVE PRACTISES
C. PROXY ARP
D. PATCHING

68. _____ PROVIDES A MECHANISM FOR REPORTING TCP/IP COMMUNICATION PROBLEMS, AS WELL AS UTILITIES FOR TESTING IP LAYER CONNECTIVITY.

A. SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)
B. INTERNET CONTROL MESSAGE PROTOCOL (ICMP)
C. CENTRALIZING ACCOUNT MANAGEMENT (AAA)
D. REMOTE COMMAND LINE

69. WHOSE FUNCTION IS TO SCREEN NETWORK TRAFFIC FOR THE PURPOSE OF PREVENTING UNAUTHORIZED ACCESS BETWEEN COMPUTER NETWORKS?

A. FIREWALLS
B. NETWORK ANALYSIS
C. DOCUMENTATION
D. NONE OF THE ABOVE

70. DIFFERENT TYPES OF SOFTWARE ADMINISTRATORS ARE CONCERNED ABOUT THAT COULD VIOLATE SECURITY POLICIES.

A. PEER-TO-PEER FILE SHARING
B. WEB MAIL
C. REMOTE ACCESS
D. ALL OF THE ABOVE

71. WHICH ONE OF THE FOLLOWING IS NOT A MUST-HAVE FIREWALL FEATURE?

A. REMOTE ACCESS
B. APPLICATION AWARENESS
C. GRANULAR APPLICATION CONTROL
D. BANDWIDTH MANAGEMENT (QOS)

72. WHICH ONE IS NOT THE CORE FUNCTION OF A FIREWALL?

A. NETWORK ADDRESS TRANSLATION

B. AUDITING AND LOGGING
C. A & B BOTH
D. NONE OF THE ABOVE

73. WHAT IS THE MASK FOR IP ADDRESS 192.168.0.0 AS PER PRIVATE ADDRESSES SPECIFIED IN RFC1918?

A. 255.0.0.0
B. 255.240.0.0
C. 255.255.0.0
D. NONE OF THE ABOVE

74. IN WHICH OF THE FOLLOWING WAY MODERN FIREWALLS ASSIST OTHER AREAS OF NETWORK QUALITY AND PERFORMANCE?

A. ENHANCE NETWORK PERFORMANCE
B. INTRUSION DETECTION AND INTRUSION PREVENTION
C. A & B BOTH
D. NONE OF THE ABOVE

75. WHICH OF THE FOLLOWING IS TRUE

A. FIREWALLS ARE USED TO RESTRICT ACCESS SPECIFIC SERVICES.
B. FIREWALL CANNOT ENFORCE SECURITY POLICIES THAT ARE ABSENT OR UNDEFINED.
C. FIREWALLS CAN ALERT APPROPRIATE PEOPLE OF SPECIFIED EVENTS.
D. ALL OF THE ABOVE

76. WHICH LAYER HOLDS THE PROTOCOLS FOR TELECOMMUNICATON?

A. NETWORK LAYER
B. PHYSICAL LAYER
C. DATA- LINK LAYER
D. TRANSPORT LAYER

77. WHICH OF THE FOLLOWING IS A FLAW OF DATA-LINK LAYER?

A. BATTERY OPERATED
B. WAR DRIVING
C. EVIL TWIN
D. ROGUE ACCESS POINT

78. THE THREATS TO DATA LINK LAYER.

A. WAR CHALKING
B. WEP CRACKING
C. BOTH A&B
D. NONE OF THE ABOVE

79. SELECT THE MITIGATION TECHNIQUE FROM THE FOLLOWING.

A. DISABLING UNUSED SERVICES
B. SWITCH SECURITY PRACTICES
C. POLICIES AND PROCEDURES
D. ALL OF THE ABOVE

80. IN WHICH OF THE FOLLOWING WAY(S) WIRELESS NETWORK SECURITY CAN BE ENHANCED

A. USE A STRONG PASSWORD
B. ENABLE YOUR ROUTER FIREWALL
C. TURN OFF GUEST NETWORKING
D. ALL OF THE ABOVE

81. WHICH OF THE FOLLOWING IS/ARE FUNDAMENTAL COMPONENT(S) OF WIRELESS INTRUSION PREVENTION SYSTEM.

A. SENSORS
B. MANAGEMENT SERVERS
C. DATABASE SERVER

UNIT 04

1. A NETWORK IDS IS REFERRED TO AS _____.
   A. HIDS B. NIDS C. SIDS D. HIPS
2. WHICH OF THE FOLLOWING IS/ARE INTRUSION DETECTION (ID) SYSTEM WHEN IT CHECKS FILES AND DISKS FOR KNOWN MALWARE?
   A. FIREWALLS B. ANTIVIRUS C. BOTH A & B D. NONE OF THE ABOVE
3. WHICH ONE OF THE FOLLOWING CANNOT BE CONSIDERED AS AN ATTACK?
   A. BUFFER OVERFLOWS
   B. DENIAL OF SERVICES
   C. PASSWORD CRACKING
   D. PATCHING
4. _____ IS AN INDEPENDENT PLATFORM THAT IDENTIFIES INTRUSIONS BY EXAMINING NETWORK TRAFFIC AND MONITORS MULTIPLE HOSTS.
   a. STACK-BASED INTRUSION DETECTION SYSTEM (SIDS)
   b. NETWORK INTRUSION DECISION SYSTEM (NIDS)
   c. HOST-BASED INTRUSION DETECTION SYSTEM (SIDS)
   d. NONE OF THE ABOVE
5. _____ IDENTIFIES INTRUSION BY ANALYZING SYSTEM CALLS, APPLICATION LOGS, FILE-SYSTEM MODIFICATIONS AND OTHER HOST ACTIVITIES.
   a. HOST-BASED INTRUSION DETECTION SYSTEM (HIDS)
   b. STACK-BASED INTRUSION DETECTION SYSTEM (SIDS)
   c. NETWORK INTRUSION DECISION SYSTEM (NIDS)
   d. ALL OF THE ABOVE
6. WHAT KIND OF AN ACTIVITY THE ATTACKS ARE CONSIDERED TO BE?
   a. ALL OF THE BELOW
   b. DENIAL OF SERVICE
   c. UNAUTHORIZED
   d. BUFFER OVERFLOW
7. WHICH OF THE FOLLOWING MEAN “FALSE POSITIVE”?
   a. INCORRECT IGNORANCE OF IMPORTANT EVENTS
   b. INCORRECT ESCALATION OF UNIMPORTANT EVENTS
   c. CORRECT IGNORANCE OF UNIMPORTANT EVENTS
   d. NONE OF THE ABOVE
8. WHICH TYPE OF SYSTEM IS AN EVOLUTION OF HIDS?
   a. STACK-BASED INTRUSION DETECTION SYSTEM
   b. NETWORK INTRUSION DECISION SYSTEM
   c. PASSIVE SYSTEM
   d. REACTIVE SYSTEM
9. WHICH SYSTEMS COMES UNDER INTRUSION PREVENTION SYSTEM (IPS)?

a. REACTIVE SYSTEMS
b. ACTIVE SYSTEMS
c. PASSIVE SYSTEMS
d. ALL OF THE ABOVE

10. WHICH OF THE FOLLOWING IS TRUE FOR INTRUSION DETECTION SYSTEM (IPS)?
    a. THEY ARE PLACED IN-LINE
    b. THEY ARE ABLE TO ACTIVELY BLOCK INTRUSIONS THAT ARE DETECTED c. TAKES ACTIONS SUCH AS SENDING AN ALARM, DROPPING THE MALICIOUS PACKETS, ETC.
    d. ALL OF THE ABOVE
11. _____ IS AN APPROACH TO SECURITY MANAGEMENT THAT COMBINES SIM (SECURITY INFORMATION MANAGEMENT) AND SEM (SECURITY EVENT MANAGEMENT). a. SIEM
    b. SOAR
    c. UEBA
    d. NONE OF THE ABOVE
12. WHICH OF THE FOLLOWING IS THE MOST IMPORTANT FEATURE TO REVIEW WHEN EVALUATING SIEM PRODUCTS?
    a. TESTING
    b. THREAT INTELLIGENCE FEEDS
    c. AGGREGATION
    d. ALL OF THE ABOVE
13. WHICH PROTOCOL IS USED FOR VOIP?
    a. SKYPE PROTOCOL
    b. MEDIA GATEWAY CONTROL PROTOCOL
    c. SESSION INITIATION PROTOCOL
    d. ALL OF THE ABOVE
14. WHICH MAIN FUNCTION IS PERFORMED BY MEDIA SERVER?
    a. PROVISIONING OF MEDIA CONNECTION
    b. VOICEMAIL FUNCTIONALITY
    c. MANAGING DIGITAL SIGNAL PROCESSING (DSP)
    d. FREE PHONE SERVICE
15. WHICH MAIN FUNCTION IS PERFORMED BY APPLICATION SERVER?
    a. SUPPORT OF CUSTOMIZED PRIVATE DIALING PLANS.
    b. SUPPORT OF BANDWIDTH POLICING MECHANISM
    c. SUPPORT OF MGCP AND MEGACO
    d. NONE OF THE ABOVE
16. _____ SWITCHES CALLS BETWEEN ENTERPRISES USERS ON LOCAL LINES WHILE ALLOWING ALL USERS TO SHARE CERTAIN NUMBER OF EXTERNAL PHONE LINES.
    a. POT
    b. PBX
    c. TEM
    d. ALL OF THE ABOVE
17. WHICH ONE OF THE FOLLOWING IS CONSIDERED TO BE IN COMPUTER SECURITY CLASSIFICATION?
    a. TYPE A
    b. TYPE D
    c. BOTH A&B
    d. NONE OF THE ABOVE
18. WHICH OF THE FOLLOWING DEFINES MICROSOFT'S TRUST WORTHY COMPUTING TECHNIQUE?
    a. MEMORY CURTAINING
    b. REMOTE ATTESTATION

c. SEALED STORAGE
d. ALL OF THE ABOVE

19. WHICH OF THE FOLLOWING IS A HARDWARE ATTACKING VECTOR?
a. BIOS
b. PBX
c. POT
d. NONE OF THE ABOVE

20. WHICH OF THE FOLLOWING DOES NOT DEFINE JERICHO SECURITY MODEL?
a. INTEGRATION
b. SIMPLIFIES USE OF PUBLIC NETWORKS
c. IT HAS A REAL OPEN SECURITY FRAMEWORK
d. AIMED FOR OPEN SOLUTION BUILDING BLOCKS

UNIT 05

1. A IS A COMPUTER FILE, TYPICALLY CALLED AN IMAGE, WHICH BEHAVES LIKE AN ACTUAL COMPUTER.

A) EXECUTABLE (EXE)
B) VIRTUAL MACHINE
C) CLOUD
D) FIREWALL

2. PROVIDED US MEANS BY WHICH WE CAN ACCESS THE APPLICATIONS AS UTILITIES OVER THE INTERNET.

A) ARTIFICIAL INTELLIGENCE
B) VIRTUAL MACHINE
C) CLOUD COMPUTING
D) INTERNET OF THINGS

3. SAAS STANDS FOR

A) SYSTEM AS A SERVICE
B) SECURITY AS A SERVICE
C) SAFETY AS A SERVICE
D) SOFTWARE AS A SERVICE

4. PROVIDES A CLOUD-BASED ENVIRONMENT WITH EVERYTHING REQUIRED TO SUPPORT THE COMPLETE LIFECYCLE OF BUILDING AND DELIVERING WEB-BASED (CLOUD) APPLICATIONS - WITHOUT THE COST AND COMPLEXITY OF BUYING AND MANAGING THE UNDERLYING HARDWARE, SOFTWARE, PROVISIONING AND HOSTING.

A) PLATFORM AS A SERVICE
B) SOFTWARE AS A SERVICE
C) INFRASTRUCTURE AS A SERVICE
D) SECURITY AS A SERVICE

5. PROVIDES COMPANIES WITH COMPUTING RESOURCES INCLUDING SERVERS, NETWORKING, STORAGE AND DATA CENTER SPACE ON A PAY-PER-USE BASIS.

A) SOFTWARE AS A SERVICE
B) INFRASTRUCTURE AS A SERVICE
C) PLATFORM AS A SERVICE
D) SECURITY AS A SERVICE

6. THE IS A DIFFERENT WAY TO BUILD PRODUCTS; IT PLACES SECURITY FRONT AND CENTER DURING THE PRODUCT OR APPLICATION DEVELOPMENT PROCESS.

A) SECURE DEVELOPMENT LIFECYCLE
B) SCRUM
C) CYBER INFRASTRUCTURE
D) SYSTEM DEVELOPMENT LIFECYCLE

7. IS THE FIRST PHASE OF SECURE DEVELOPMENT LIFECYCLE (SDL).

A) IMPLEMENTATION OR CODING
B) DESIGN PHASE
C) TEST PHASE
D) REQUIREMENTS PHASE

8. WAF STANDS FOR.

A) WIRELESS APPLICATION FIREWALL
B) WEB APPLICATION FIREWALL
C) WEB APPLICATION FACTOR
D) WIRED APPLICATION FIREWALL

9. WEB APPLICATION COOKIES SHOULD NOT CONTAIN USERS'.

A) USERNAME
B) EMAIL ADDRESS
C) CONTACT NUMBER
D) PASSWORD

10. IT IS A BENEFICIAL TO RUN WEB APPLICATIONS USING PRIVILEGES.

A) LEAST
B) MOST
C) MEDIUM
D) ADMINISTRATIVE

11. CLIENT APPLICATIONS ARE WEB-BASED APPLICATION WHICH CAN BE ACCESSED ON THE INTERNET USING A BROWSER.

A) THICK
B) CLOUD
C) COMPUTING
D) THIN

12. THICK CLIENT APPLICATIONS PEFORM MAJOR PROCESSING ON THE.

A) SERVER SIDE

B) CLOUD
C) CLIENT SIDE
D) VIRTUAL MACHINE

13. THIN CLIENT APPLICATIONS DO NOT OCCUPY ANY SPACE ON THE.

A) SERVER SIDE
B) CLIENT SIDE
C) CLOUD
D) VIRTUAL MACHINE

14. WHICH VULNERABILITY AMONG THESE IS APPLICABLE FOR BOTH THIN CLIENT AND THICK CLIENT APPLICATIONS?

A) CROSS SITE SCRIPTING
B) CLICKJACKING ATTACKS
C) REVERSE ENGINEERING
D) IMPROPER ERROR HANDLING

15. USING A SYSINTERNAL TOOL CALLED, WE CAN IDENTIFY THE FILES AND REGISTRIES USED BY A PARTICULAR THICK CLIENT APPLICATION.

A) AUTOLOGON
B) PROCESS MONITOR
C) MOVEFILE
D) TCPVIEW

16. IS AN ADVANCED MONITORING TOOL FOR WINDOWS THAT SHOWS REAL-TIME FILE SYSTEM, REGISTRY AND PROCESS/THREAD ACTIVITY.

A) PROCESS MONITOR
B) FILE MONITOR
C) WIRESHARK
D) SERVICE MONITOR

17. WHICH OF THESE IS NOT A WEB APPLICATION ATTACK?

A) SQL INJECTION
B) CROSS SITE SCRIPTING
C) ADDRESS RESOLUTION PROTOCOL (ARP) POISONING
D) SESSION HIJACKING

18. RDP STANDS FOR.

A) REMOTE DATA PROTOCOL
B) REMOTE DESKTOP PROTOCOL
C) RELIABLE DESKTOP PROTOCOL
D) REMOTE DATABASE PROTOCOL

19. REMOTE DESKTOP PROTOCOL (RDP) SESSIONS OPERATE OVER CHANNEL, PREVENTING ANYONE FROM VIEWING YOUR SESSION BY LISTENING ON THE NETWORK.

A) BROADCAST
B) UNENCRYPTED
C) ENCRYPTED
D) OPEN

20. IT IS A GOOD SECURITY MEASURE TO USE TO RESTRICT ACCESS TO REMOTE DESKTOP LISTENING PORTS.

E) FIREWALL
F) ANTIVIRUS
G) ENCRYPTION
H) INTRUSION DETECTION SYSTEM (IDS)

21. NLA STANDS FOR.

A) NETWORK LAYER ACCESS
B) NETWARE LOG ANALYZER

C) NETWORK LEVEL AUTHENTICATION
D) NETWORK LAYER AUTHORIZATION

22. FOR PREVENTING BRUTE-FORCE ATTACK ON REMOTE DESKTOP PROTOCOL (RDP), IS THE MOST EFFECTIVE WAY.

A) SERVER LOG MONITORING
B) SINGLE FACTOR AUTHENTICATION
C) ACCOUNT LOCKOUT POLICY
D) DETERRENCE MECHANISM

23. NAP STANDS FOR, WHICH IS USED WITH REMOTE DESKTOP (RD) GATEWAY.

A) NETWORK ADDRESS PROTECTION
B) NET ACCESS PROTOCOL
C) NEW ADDRESS PROTOCOL
D) NETWORK ACCESS PROTECTION

24. IS THE PROTECTION OF PERSONNAL, HARDWARE, SOFTWARE, NETWORKS AND DATA FROM PHYSICAL ACTIONS AND EVENTS THAT COULD CAUSE SERIOUS LOSS OR DAMAGE TO AN ENTERPRISE, AGENCY OR INSTITUTION.

A) CLOUD SECURITY
B) PHYSICAL SECURITY
C) NETWORK SECURITY
D) APPLICATION SECURITY

25. EFFECTIVE PHYSICAL SECURITY OF AN ASSET IS ACHIEVED BY MULTI-LAYERING THE DIFFERENT MEASURES, WHICH IS COMMONLY REFERRED TO AS.

A) DEFENSE IN DEPTH
B) ENCRYPTION
C) DISASTER RECOVERY
D) DATA BACKUP

26. IS SOMETHING USEFUL OR VALUABLE THING TO AN ORGANIZATION.

A) SECURITY
B) REVENUE
C) ASSET
D) INFRASTRUCTURE

27. OUTLINE THE QUALITIES OF AN ASSET THAT ARE IMPORTANT TO PROTECT.

A) SECURITY REPORT

B) SECURITY REQUIREMENTS
C) SECURITY DESIGN
D) SECURITY TEST

28. C IN THE CIA TRIAD STANDS FOR.

A) CONNECTION
B) CONTROL
C) CONFIGURATION
D) CONFIDENTIALITY

29. RFID STANDS FOR, WHICH IS USED AS AN ACCESS MECHANISM FOR SECURING ASSETS.

A) REQUEST FOR IMPLEMENTATION DATA
B) RADIO FREQUENCY IDENTIFICATION
C) REPEATED FREE INDUCTION DECAY
D) REQUEST FOR IMPLEMENTATION DATE

30. IS A METHOD/TECHNIQUE USED BY AN UNAUTHORIZED PERSON WHO ENTERS THE PREMISES BY FOLLOWING THE AUTHORIZED PERSON.

A) PHISHING
B) BAITING
C) TAILGATING
D) SMISHING

31. CCTV STANDS FOR, WHICH ARE USED IN ELECTRONIC MONITORING FOR SECURING ASSETS.

A) CLOSED CIRCUIT TELEVISION
B) CAPITAL COMMUNITY TELEVISION
C) CAMPZONE COMMUNITY TELEVISION
D) COMMAND AND CONTROL TELEVISION

32. IS A TECHNOLOGY FOR MEASURING AND ANALYZING BIOLOGICAL DATA OF A HUMAN BODY SUCH AS FINGERPRINTS, EYE RETINAS, VOICE PATTERNS, ETC.

A) MOTION SENSOR
B) CCTV
C) BIOMETRICS
D) RFID READER

33. IS A PATTERN RECOGNITION SYSTEM WHERE A BIOLOGICAL PATTERN IS ANALYZED, MATCHED AND PROCESSED FOR FURTHER ACTIONS.

A) DISCRIMINANT ANALYSIS
B) BIOMETRIC SYSTEM
C) SIGNAL PROCESSING
D) PREDICTIVE ANALYSIS

34. WHAT IS THE FIRST STEP IN A BIOMETRIC SYSTEM?

A) PROCESSING
B) ANALYZING
C) ENROLLMENT
D) RECOGNITION

35. IN BIOMETRICS, THICKNESS AND LOCATION OF VEINS IN A PERSON'S HAND ARE USED AS FEATURES.

A) SIGNATURE
B) HAND
C) IRIS
D) VASCULAR PATTERN

36. ARE USED IN DATA CENTERS TO ALERT ABOUT TEMPERATURE CHANGES, WATER LEAKEAGES, HUMIDITY INCREASES, ETC.

A) INTRUSION DETECTION SYSTEM (IDS)
B) PROGRAMMABLE LOCKS
C) MOTION SENSORS

D) ELECTRIC FENCES

37. ARE THOSE INFORMATION-RELATED ASSETS THAT WOULD CAUSE A LARGE ADVERSE IMPACT ON THE ORGANIZATION IF THEY ARE DISCLOSED TO UNAUTHORIZED PEOPLE.

A) CRITICAL ASSETS
B) INVENTORY ASSETS
C) OPERATING ASSETS
D) NON-CURRENT ASSETS

38. WHICH IS AN IMPORTANT FACTOR TO CONSIDER WHEN SELECTING A NEW LOCATION FOR SECURITY?

A) POPULATION
B) COMPETITION
C) POLLUTION
D) ENVIRONMENT

39. THE UNAUTHORIZED DISCLOSURE OF TYPE OF ASSETS CAN CAUSE GRIEVOUS DAMAGE TO THE NATIONAL SECURITY

A) CONFIDENTIAL
B) TOP SECRET
C) UNCLASSIFIED
D) SECRET

40. AMAZON WEB SERVICES (AWS) AND MICROSOFT AZURE CLOUD ARE EXAMPLES OF.

A) SOFTWARE AS A SERVICE
B) PLATFORM AS A SERVICE
C) SYSTEM AS A SERVICE
D) INFRASTRUCTURE AS A SERVICE