The Bodwad Sarvjanik co-op, Education Society Ltd,Bodwad

Arts Commerce Science College Bodwad

Question Bank

Class:-SyBsc Sem:- iv

Paper Name:-Network security(skill enhancement course) Subject:- CS-404

1.To check the integrity of a message, or document, the receiver creates the A.hash-table **B.hash tag** C.hyper text D. finger print

2.A digital signature needs a

A.private-key system

B.shared-key system

C.public-key system

D.secret key

3.One way to preserve the integrity of a document is through the use of a

A.eye-rays **B.finger print**

C.biometric D. X-Rays

4.A session symmetric key between two parties is used

A.only once B.twice

C.multiple times D. conditions dependant

5.Encryption and decryption provide secrecy, or confidentiality, but A.authentication **B.integrity** C.privacy D. modularity

6.Confidentiality with asymmetric-key cryptosystem has its own

A.entities B.data **C.problems** D.translator

7.Secure Hash Algorithm 1 (SHA-l) has a message digest of

A.160 bits B.512 bits C.628 bits D.820 bits

8.Message authentication is a service beyond A.Message confidentiality **B.message integrity** C.message splashing D.message sending

9.In message confidentiality, the transmitted message must make sense to only intended **A.receiver** B.sender C.modulor D.translator

10.A hash function guarantees the integrity of a message. It guarantees that the message has not be A.replaced B.over view **C.changed** D. violated

11.MAC stands for

A.message Authentication Code

B.Message Arbitrary Connection

C.Message Authentication Control

D.Message Authentication Cipher

12.The digest created by a hash function is normally called a

A.modification detection code (mdc)

B.modify authentication connection

C. message authentication control

D.message authentication cipher

13.Message confidentiality is using

A.cipher text B.cipher C.symmetric-key **D.asymmetric-key**

14.A sender must not be able to deny sending a message that was sent, is known as

A.message nonrepudiation

B.message integrity
C.message confidentiality D.message sending
15.To preserve the integrity of a document, both the document and the fingerprint are
A.not used B.unimportant **C.needed** D.not needed
16.When the data must arrive at the receiver exactly as they were sent, its called
A.message confidentiality **B. message integrity**
C. message splashing D.message sending
17.The message digest needs to be
A.public B.private **C.kept secret** D.integerity
18.In message integrity, the message digest needs to be kept
A.secret B.low C.high D.constant 0
19.In Message Integrity, Secure Hash Algorithm 1 (SHA-l) hash algorithms create an N-bit message-digest out of a message of
A.512 bit blocks B.1001 bit blocks
C.1510 bit blocks D.2020 bit blocks
20.The Message confidentiality or privacy means that the sender and the receiver expect
A.integrity **B.confidentiality**
C.authentication D.nonrepudiation
21.The message must be encrypted at the sender site and decrypted at the A. sender site B.site **C.receiver site** D.conferencing
22. In brute force attack, on average half of all possible keys must be tried to achieve success.
A.True B.False
23.If the sender and receiver use different keys, the system is referred to as a conventional cipher system.
A.True **B.False**
24. Divide (HAPPY)26 by (SAD)26. We get quotient –
A.KD B.LD C.JC D.MC
25.Dividing (11001001) by (100111) gives remainder – A.11
B.111 C.101 **D.110**
26.pi in terms of base 26 is
A. C.DRS B. D.SQR
C. D.DRS D. D.DSS
27.The time required to convert a k-bit integer to its representation in the base 10 in terms of big-O notation is **A. O(log2 n)**
B.O(log n) C.O(log2 2n) D.O(2log n)
28. In base 26, multiplication of YES by NO gives – A.THWOE
B.MPAHT **C.MPJN** D.THWAE
29.Division of (131B6C3) base 16 by (lA2F) base 16 yeilds – A.1AD B.DAD C.BAD **D.9AD**
30.An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available.
A.True B.False
31.The estimated computations required to crack a password of 6 characters from the 26 letter alphabet is- A**.308915776**
B. 11881376 C.456976 D. 8031810176

32. DES follows A. Hash Algorithm B.Caesars Cipher **C.Feistel Cipher Structure** D.SP Network

33.The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key A.12 B.18 C.9 **D.16**

34.The DES algorithm has a key length of A.128 Bits B.32 Bits **C. 64 Bits** D. 16 Bits

35. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.

A.True **B.False**

36.In the DES algorithm the round key is _____ bit and the Round Input is _____bits.

A.48, 32 B.64,32 C.56, 24 D. 32, 32

37. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____

A.Scaling of the existing bits B.Duplication of the existing bits C.Addition of zeros D.Addition of ones

38.The Initial Permutation table/matrix is of size A.16×8

B. 12×8 C.**8×8** D.4×8

39.The number of unique substitution boxes in DES after the 48 bit XOR operation are **A.8** B.4 C.6 D.12

40. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.

A.True **B. False**

41.First boot sector virus is

A.Computed B.Mind **C.Brain**

D.Elk cloner

42.The linking of computers with a communication system is called

A. Assembling B.Interlocking

C.Pairing **D.Networking**

43.The phrase ____ describe viruses, worms, Trojan horse attack applets and attack scripts.

A.Spam B.Phishing **C.Malware**

D.Virus

44.Abuse messaging systems to send unsolicited is A.Phishing

B.Adware C.Firewall **D.Spam**

45.A person who uses his or her expertise to gain access to other people's computers to get information illegally or do damage is a **A.Hacker** B.Analyst C.Spammer D.Programmer

46.What type of symmetric key algorithm using a streaming cipher to encrypt information?

A. RC4 B. Blowfish C. SHA D. MD5

47.Which of the following is not a factor in securing the environment against an attack on security?

A. The education of the attacker

B. The system configuration

C. The network architecture

D. The business strategy of the company

E. The level of access provided to employees

48. What type of attack uses a fraudulent server with a relay address?

A. NTLM **B. MITM** C. NetBIOS

D. SMB
49.What port is used to connect to the Active Directory in Windows 2000?
A. 80 B. 445 C. 139 **D. 389**
50.To hide information inside a picture, what technology is used?
A. Rootkits B. Bitmapping
C. Steganography D. Image Rendering
51.Which phase of hacking performs actual attack on a network or system?
A. Reconnaissance B. Maintaining Access C. Scanning **D. Gaining Access**
52.Attempting to gain access to a network using an employee's credentials is called the _____ mode of ethical hacking.
A. Local networking B. Social engineering C. Physical entry
D.Remote networking
53. The field that covers a variety of computer networks, both public and private, that are used in everyday jobs.
A.Artificial Intelligence B.ML
C.Network Security D.IT
54. Network Security provides authentication and access control for resources.
A.True B.False
55. Which is not an objective of network security?
A.IdentificationB.Authentication C.Access control **D.Lock**
56. Which of these is a part of network identification?
A.UserID B.Password C.OTP D.fingerprint
57. The process of verifying the identity of a user.
A.Authentication B.Identification
C. Validation D.Verification
58.A concern of authentication that deals with user rights.
A.General access
B.Functional authentication
C.Functional authorization
D.Auto verification
59.CHAP stands for?
A.Challenge Handshake authentication protocol
B.Challenge Hardware authentication protocol
C.Circuit Hardware authentication protocol
D.Circuit Handshake authentication protocol
60. Security features that control that can access resources in the OS.
A.Authentication B.Identification
C.Validation **D.Access control**
61.An algorithm in encryption is called _____
A.Algorithm B.Procedure
C.Cipher D.Module
62. The information that gets transformed in encryption is _____
A.Plain text B.Parallel text
C.Encrypted text D.Decrypted text
63. Which malicious program cannot do anything until actions are taken to activate the file attached by the malware.
A.Trojan horse B. Worm **C.virus**
D. Bots

64. Which of the following is not a stand alone program?
A.Trojan **B.worm** C.virus D.spyware
65. A Firewall needs to be – – so that it can grow with the network it protect A. Robust **B.Expensive**
C. Fast D. Scalable
66. A proxy Firewall filter at at A.physical layer B.data link layer
C. network layer **D.application layer**
67. Which of the following is not a valid access control mechanism?
A.DAC **B.SAC** C. MAC. D. RBAC
68. Stateful wire fall maintains a – – which is a list of active connections?
A.Routing table B.state table
C.bridging table D. Connection table
69. The virus is a computer ----
A.network B.database
C.file **D. Program**
70. The ----- attacks is related to confidentiality.
A.modification B.fabrication C.interruption **D. Interception**
71. Which of the following is not a security?
A.Authentication B.Cross site scripting C. SQL injection
D.eavesdropping
72. When services of network or server are inaccessible to user attack is known as
A.snooping
B. interception C.snooping **D.Denial of services**
73. Encryption is the technique in which message is converted in ----form A.plaintext **B.scramble**
C.clear D.none of these
74. A Firewall is installed at the point where the secure internal Network and untrusted external network meet which is also known as
A. chock point B.meeting point
C. Firewall point D.secure point
75. What are the uses of Malware?
A.many early infectious programs, including the first Internet worm ,were written as experiments or pranks
B. Today Malware is used Primarily to steal sensitive personal,financial or business information for the benefit of others
C. All of these
D. Malware is sometimes used broadly against the government or corporate websites to gather guarded information or to disrupt their operation in general
76. There are ---- types of dos attack.
A.4 B.5 **C.2** D.3
77. Which method of hacking will record all your keystrokes?
A.keylogging B.keyjacking
C.keyhijacking D.keyboard monitoring
78. Which of the following is not a type of Cyber attack attack
A.bad password **B.Murder**
C.spoofing D.snuffing
79. Intercepting between two points means
A.key logger attack B.bad password attack C.program flow attack

D. Eavesdropping attack

80.What are the major components of the intrusion detection system?

A.Analysis Engine B.Event provider

C. Alert Database

D. All of the mentioned

81.What are the major components of the intrusion detection system?

A.Analysis Engine B.Event provider C.Alert Database **D.All of the mentioned**

82. Dos attacks are caused by ----

A. authentication B.alteration

C.fabrication **D.reply attack**

83. If the recipient of a message have to be satisfied with the identity of the sender the principle -----comes into the picture.

A.integrity **B.authentication**

C.access control D.confidentiality

84. What are the different ways to classify an IDS?

A.Zone based

B.Host & Network based

C.Network & Zone based

D.Level based

85.Who deploys malwares to a system aur network?

A.three mineral organisation white hat hacker Malware developers cyber terrorist

B.criminal organisation Black hat hacker Malware developers cyber terrorist

C.criminal organisation Black hat hacker software developer cyber terrorist

D.criminal organisation grey hat hacker Malware developers, penetration testers

86. DDoS stands for -----

A.direct distribution of service

B.distributed denial of server

C.direct distribution of server

D. distributed denial of service

87. Sniffing is also known as ----

A.network tapping B.net typing

C.wireless tapping **D.wiretapping**

88. What are the types of Malware? A.caterpillar **B.worms** C.lions

D.horses

89. What is an antivirus?

A.computer software used to prevent ,detect and remove malicious software

B.a bigger and more dangerous virus C.a Biological agent that reproduces itself inside the cells of living things D.software used to duplicate viruses

90. What are the different ways to classify an IDS?

A.Zone based **B.Host & Network based** C.Network & Zone based D.Level based

91. Network layer firewall works as a _____ A.Frame filter

B.Packet filter C.Content filter

D.Virus filter

92. Network layer firewall has two sub-categories as _____

A.State full firewall and stateless firewall

B.Bit oriented firewall and byte oriented firewall

C.Frame firewall and packet firewall

D.Network layer firewall and session layer firewall

93. What are the different ways to classify an IDS?
A.anomaly detection B.signature based misuse C.stack based
D.all of the mentioned
94.A worm ---modify a program.
A. Does B. May or may not
C. Does not D. May
95. Which of the following is / are the types of firewall?
A.Packet Filtering Firewall
B.Dual Homed Gateway Firewall
C.Screen Host Firewall
D.Dual Host Firewall
96.A --- tries to formulate a web resources occupied Or busy it's users by flooding the URL of the victim with unlimited request than the server can handle.
A.MiTM attack B. website attack
C.phishing attack **D. Dos attack**
97. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____
a) Chock point B.Meeting point
C.Firewall point D.Secure point
98. Attack controlling user program means **A.program flow attack**
B.bad password attack
C.snuffing attacks
D. Spoofing attack
99. What are the different ways to classify an IDS?
A.anomaly detection B.signature based misuse C.stack base **D.all of the mentioned**
100.What are the characteristics of anomaly based IDS?
A.It models the normal usage of network as a noise characterization
B. It doesn't detect novel attacks
C.Anything distinct from the noise is not assumed to be intrusion activity
D.It detects based on signature
----------Best of Luck----------