CWIPEDIA.IN

Question Bank 2

1. Which of the following are possible security threats?

A. Illegitimate use
B. Backdoors
C. Masquerading
D. All Of The Given Options Are Correct

D. All of the given options are correct

2. What is a firewall?

A. Firewalls Are Network-Based Security Measures That Control The Flow Of Incoming And Outgoing Traffic
B. A firewall is a program that encrypts all the programs that access the Internet.
C. A firewall is a program that keeps other programs from using the network.
D. Firewalls are interrupts that automatically disconnect from the internet when a threat appears

A. Firewalls are network-based security measures that control the flow of incoming and outgoing traffic

3. Which of the following involves submitting as many requests as possible to a single Internet computer or service, overloading it and preventing it from servicing legitimate requests?

A. Distributed Denial-Of-Service Attacks
B. Backdoor
C. Masquerading

D. Phishing

A. Distributed denial-of-service attacks

4. Which of the following symmetric keys can be derived from Symmetric master key?

A. Authentication keys
B. Key wrapping keys
C. Data encryption keys
D. All Of The Given Options Are Correct

D. All of the given options are correct

5. Which of the following are valid Cryptographic key types?

A. Public authentication key
B. Public signature verification key
C. Private signature key
D. All Of The Given Options Are Correct

D. All of the given options are correct

6. Is true that HTTP is an insecure protocol?

A. True
B. False

A. True

7. Which is the best way a system can be hardened?

A. Total Disk Encryption Coupled With Strong Network Security Protocols.
B. White-list ad filtering only.
C. Installing a commercial security suite.
D. Virus scanning only.

A. Total disk encryption coupled with strong network security protocols.

8. Why is it crucial to encrypt data in transit?

A. To assure that all of your information cannot be decrypted.
B. To decrease your resources.
C. So you can increase your chances of testing your encryption capabilities.
D. To Prevent Unauthorized Access To Private Networks And Sensitive Information During Its Most Vulnerable State.

D. To prevent unauthorized access to private networks and sensitive information during its most vulnerable state.

9. Which of the following are the basic functionalities of the IPsec Protocol ?

A. Security association for policy management and traffic processing
B. Security protocols for AH and ESP
C. Manual and automatic key management for the internet key exchange
D. All Of The Given Options Are Correct

D. All of the given options are correct

10. Can a proxy be used as a firewall? If so, how?

A. No. Proxies are data encryption stations whose sole purpose is to encrypt and re-rout data.
B. No. Proxies are firewalls that are maintained at locations other than that of the user.
C. No. All a proxy does is re-rout Internet traffic, and thus all the malicious signals that go with it.
D. Yes. A Proxy Acts As A Network Intermediary For The User That Serves To Control The Flow Of Incoming And Outgoing Traffic.

D. Yes. A proxy acts as a network intermediary for the user that serves to control the flow of incoming and outgoing traffic.

11. In which of the following fraud methods is a legitimate/legal-looking email sent in an attempt to gather personal and financial information from recipients?

A. Virus
B. Masquerading
C. Phishing
D. Malware

C. Phishing

12. Which of the following is TRUE about TLS?

A. The HMAC construction used by most TLS cipher suites is specified in RFC 2104
B. Provides protection against a downgrade of the protocol to a previous (less secure) version or a weaker cipher suite
C. The message that ends the handshake sends a hash of all the exchanged handshake messages seen by both parties

D. All Of The Given Options Are Correct

D. All of the given options are correct

13. Which of the following is a VALID type of Key Management System?

A. Third-Party Key Management System
B. Dynamic Key Management System
C. Integrated Key Management System
D. Both Integrated Key Management System And Third-Party Key Management System

D. Both Integrated Key Management System and Third-Party Key Management System

14. What is one way that a web browser is vulnerable to breaching?

A. A browser can be infected by closing it.
B. A virus can be sent through the monitor.
C. A Browser Plugin Can Be Exploited.
D. Web browsers are impervious to exploitation.

C. A browser plugin can be exploited.

15. What two main categories of network topologies are there?

A. Digital and Topological
B. Direct and Indirect
C. Close and Distant
D. Physical And Logical.

D. Physical and logical.

16. What is another name for an insecure plugin?

A. Hardware
B. Software
C. Firmware
D. Malware

D. Malware

17. A digital signature scheme consists of which of the following typical algorithms?

A. Key Generation, Signing And Signature Verifying Algorithm
B. Signature verifying algorithm
C. Key generation algorithm
D. Signing algorithm

A. Key generation, Signing and Signature verifying algorithm

18. Which of the following is TRUE about SSL 3.0?

A. It has a weak MAC construction that uses the MD5 hash function with a secret prefix
B. Identical cryptographic keys are used for message authentication and encryption
C. SSL 3.0 Improved Upon SSL 2.0 By Adding SHA-1 Based Ciphers And Support For Certificate Authentication
D. It assumes a single service and a fixed domain certificate, which clashes with the standard feature of virtual hosting in Web servers

C. SSL 3.0 improved upon SSL 2.0 by adding SHA-1 based ciphers and support for certificate authentication

19. There are two types of firewall. What are they?

A. Internet-based and home-based.
B. Hardware And Software.
C. Remote and local
D. Digital and electronic.

B. Hardware and software.

20. True of False? Malware exists which affects both Windows and Linux systems.

A. True
B. False

A. True

21. Which of the following refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent?

A. Malware
B. Botnet
C. Trojan horse
D. Spyware

D. Spyware

22. What is a computer worm?

A. It is software designed to exploit networks.
B. It is software designed to analyze and search for open ports.
C. It is a software utilized to scan packets on open networks.
D. It Is Malware Designed To Infect Other Computers.

D. It is malware designed to infect other computers.

23. Is a Unix-based system vulnerable to viruses?

A. Yes. The split is approximately 50/50 when it comes to attacks on Windows vs. Unix based systems.
B. Yes, the majority of viruses attack Unix-based systems.
C. No. Linux systems are totally impervious to attacks.
D. Yes, However The Majority Are Coded To Attack Windows-Based Systems.

D. Yes, however the majority are coded to attack Windows-based systems.

24. Which of the following protocol used Port 443 and Port 80 respectively

A. HTTPS And HTTP
B. XHTML
C. HTTP and HTTPS
D. DHTML

A. HTTPS and HTTP

25. Which of the following is a means to access a computer program or entire computer system bypassing all security mechanisms?

A. Backdoor
B. Masquerading
C. Phishing
D. Trojan Horse

A. Backdoor

26. What does TCP mean?

A. Total Content Positioning
B. Transmission Control Protocol
C. Transmittable Constant Protocol
D. Technical Control Panel

B. Transmission Control Protocol

27. What does cross-site scripting allow for attackers?

A. Direct introduction of viruses into a victims computer.
B. The introduction of worm viruses into the victims website.
C. A phishing attack that automatically downloads the victims personal information.
D. Injection Of Client-Side Scripts Into Web Pages.

D. Injection of client-side scripts into web pages.

28. Which of the following is collection of Internet-connected programs communicating with other similar programs in order to perform tasks?

A. Botnet
B. Spyware
C. Trojan horse

D. Malware

A. Botnet

29. What are TLS and SSL?

A. Internet protocols.
B. Network layers.
C. Internet layers
D. Cryptographic Protocols.

D. Cryptographic protocols.

30. Who was TLS defined by?

A. The DEA
B. OSHA
C. Internet Engineering Task Force
D. NSA

C. Internet Engineering Task Force

31. Modern secure password storage should implement:

A. Salted plain-text values of the password
B. Hashed values of the password
C. Plain-text passwords stored in an encrypted database
D. Salted And Hashed Values Of The Password

D. Salted and hashed values of the password

32. What is network topology?

A. It is the inner networkings of a single computer.
B. It is the top layer of a computer network.
C. It Is The Framework Of The Components Of A Computer Network.
D. It is the entirety of the data of a computer network.

C. It is the framework of the components of a computer network.

33. Which of the following is a general term for malicious software that pretends to be harmless so that a user willingly allows it to be downloaded onto the computer?

A. Spware
B. Virus
C. Trojan Horse
D. Botnets

C. Trojan Horse

34. What is another name for Internet Layer?

A. TCP layer
B. Interwebs
C. IP Layer
D. SSL layer

C. IP layer

35. Which of the following is the collective name for Trojan horses, spyware, and worms?

A. Spware
B. Botnets
C. Virus
D. Malware

D. Malware

36. When cookies are used as session identifiers, how are they then used as a potential security hazard?

A. They emulate user's by downloading all the victims information onto a virtual machine.
B. User's cookies are altered to a virus-like state.
C. They emulate user's by stealing their personal identity.
D. Attackers Emulate Users By Stealing Their Cookies.

D. Attackers emulate users by stealing their cookies.

37. Which of the following is a valid flaw of SSL 2.0 ?

A. It does not have any protection for the handshake
B. Identical cryptographic keys are used for message authentication and encryption
C. It has a weak MAC construction that uses the MD5 hash function with a secret prefix
D. All Of The Given Options Are Correct

D. All of the given options are correct

38. Which of the following is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI)?

A. X.507
B. X.519
C. X.508
D. X.509

D. X.509

39. Trojan Horse programs operate with what intent?

A. To slowly but surely infect and become your operating system until the system crashes.
B. To openly exploit a systems weaknesses until the user discovers it.
C. To Masquerade As Non-Malicious Software While Exploiting A System's Weaknesses.
D. To do a series of brute force attacks within the system itself and a series of external attacks from other servers

C. To masquerade as non-malicious software while exploiting a system's weaknesses.

40. Why is a virtual machine considered a sandboxing method?

A. Virtual machines all have firewalls, virus scanners, and proxy connetions.
B. Virtual machines all have sandbox features installed on them.
C. Virtual machines take the brunt of the attack, so the user is always safe.
D. All Host Resources Are Channeled Through The Emulator.

D. All host resources are channeled through the emulator.

41. When is encrypted data the safest?

A. When it is being transferred via usb stick.
B. When it is in transit.
C. When It Is Being Written. When It Is At Rest.
D. When it is being written.

C. When it is being written. When it is at rest.

42. Which of the following keys are used to generate random numbers?

A. Symmetric random number generation keys
B. Symmetric And Asymmetric Random Number Generation Keys
C. Public signature verification key
D. Asymmetric random number generation keys

B. Symmetric and asymmetric random number generation keys

43. Which of the following is true about Public Key Encryption?

A. Anyone can encrypt with the public key and anyone can decrypt with the private key
B. Anyone Can Encrypt With The Public Key, Only One Person Can Decrypt With The Private Key
C. Anyone can encrypt with the private key, only one person can decrypt with the public key
D. Only one person can encrypt with the public key and anyone can decrypt with the private key

B. Anyone can encrypt with the public key, only one person can decrypt with the private key

44. If you set up a BUS network, what is the major disadvantage?

A. It is entirely wireless and open to wifi-based attacks.
B. It is daisy-chained together with several cables
C. It Is Linked With A Single Cable Which Can Be A Major Vulnerability.
D. It is connected in a star pattern and can be disabled by disrupting one data center.

C. It is linked with a single cable which can be a major vulnerability.

45. What does the acronym BEAST mean in Beast Attack?

A. Breaking and Entering Against SSL/TLS
B. Browser Extension And SSL/TLS
C. Browser Exploit Against SSL/TLS
D. Breach Entering Against SSL/TLS

C. Browser Exploit Against SSL/TLS

46. TCP is used for what three main functions?

A. Connect To The Web, Deliver Email, And Transfer Files.
B. Connect to the Web, compress data, encrypt mail.
C. Connect to the web, conceal data, transfer files.
D. Connect to the Web, encrypt data, transmit information.

A. Connect to the Web, deliver email, and transfer files.

47. Secure cookies have which feature?

A. They are not encrypted, just sent via secure server.

B. They Are Encrypted.
C. Secure cookies are passed along via encrypted programs.
D. Cookies are always traded between trusted users.

B. They are encrypted.

48. How are port numbers categorized?

A. Static, dynamic, enigmatic
B. Known, well-known, unknown
C. Well-Known, Registered, And Static/Dynamic.
D. Unknown, unregistered, invalid

C. Well-known, registered, and static/dynamic.

49. Which of the following type of attack can actively modify communications or data?

A. Both Active and Passive attack
B. Neither Active nor Passive attack
C. Active Attack
D. Passive attack

C. Active attack

50. What is the top method an attacker might infect a target?

A. Social Engineering, Or Psychological Manipulation.
B. SQL injection.
C. Buffer overflow.
D. Hacking via the Internet.

A. Social engineering, or psychological manipulation.

51. Secure Sockets Layer is a predecessor of which cryptographic protocol?

A. IPSec
B. Transport Layer Security
C. SSL 3.0
D. HTTPS

B. Transport Layer Security

52. An SQL injection is often used to attack what?

A. Small scale machines such as diebold ATMs
B. Large-Scale Sequel Databases Such As Those Containing Credit Card Information.
C. Servers running SQL databases similar to Hadoop or Hive.
D. Servers built on NoSQL

B. Large-scale sequel databases such as those containing credit card information.

53. Which version of TLS is vulnerable to BEAST exploit?

A. TLS 1.1
B. TLS 3.0
C. TLS 0.5
D. TLS 2.0
E. TLS 1.0

E. TLS 1.0

54. According to OWASP what is the most dangerous web vulnerability?

A. Injections (SQL, LDAP, Etc)
B. Cross-site-scripting (XSS)
C. Security Misconfiguration
D. Cross-Site Request Forgery (CSRF)
E. Sensitive Data Exposure

A. Injections (SQL, LDAP, etc)

55. Sandboxing does what to computer programs?

A. Sandboxing protects your system by trapping all the viruses.
B. It Separates And Isolates Them.
C. Sandboxing doesn't protect your system.
D. Sandboxes protect your programs by isolating all the other programs except the one you are using at the time.

B. It separates and isolates them.

56. What is largely considered the most advanced computer virus?

A. Conficker Virus
B. Zeus
C. Stuxnet.
D. agent.biz

C. Stuxnet.

57. What is necessary for a cross-site script attack with cookies to be thwarted?

A. CAPTCHAs
B. Virtual machines
C. Proxies
D. Firewalls

A. CAPTCHAs

58. What are the two primary classifications of cross-site scripting?

A. DOM-based and persistent
B. traditional and DOM-based
C. traditional and non-persistent
D. Non-Persistent And Persistent.

D. non-persistent and persistent.

59. Which of the following is a VALID authorization key?

A. Public Authorization Key
B. Public ephemeral key authorization key
C. Asymmetric authorization keys
D. Symmetric authorization keys

A. Public authorization key

60. Which of the following is a VALID digital signature key?

A. Public signature authentication key
B. Private signature authentication key
C. Symmetric signature authentication key

D. Private Signature Key

D. Private signature key

61. How can cookies be used to mitigate cross-site scripting?

A. Cookies can be coded like a program to intercept script attacks.
B. Cookies store an exact mirror copy of all a users web activity.
C. Cookies Allow For Cookie-Based User Authentication.
D. They can't. Cookies only store user information.

C. Cookies allow for cookie-based user authentication.

62. Which of the following uses asymmetric cryptography ?

A. VoIP
B. SSL
C. Both VoIP And SSL
D. None of these

C. Both VoIP and SSL

63. Which of the following is not a VALID type of firewall?

A. Application-level gateways
B. Circuit-level gateways
C. Proxy Server Gateways
D. Packet filters

C. Proxy Server Gateways

64. What is the less secure AES encryption mode?

A. CFB
B. OCB
C. ECB
D. CTR
E. CBC

E. CBC

65. What is a method to fend off a Sockstress attack?

A. Do nothing. It will pass on its own.
B. Prepare a retaliatory DDOS attack
C. Black-listing access to TCP services on critical systems
D. White-Listing Access To TCP Services On Critical Systems.

D. White-listing access to TCP services on critical systems.

66. Which of the following HTTP method is considered insecure ?

A. POST
B. DELETE
C. TRACE
D. GET

C. TRACE

67. Which of the following represents a cryptographic key that is generated for each execution of a key establishment process ?

A. Private key transport key

B. Public signature verification key
C. Private Ephemeral Key Agreement Key
D. Public authentication key

C. Private ephemeral key agreement key

68. What does the Linux kernal use to sandbox running programs?

A. Linux doesn't sandbox because it is impervious to any and all cyber attacks
B. Linux uses a layered system of user authentication to perform sandbox-like functions.
C. Seccomp, Or Secure Computing Mode
D. Linux drives are fully encrypted, thus they don't need sandboxing.

C. seccomp, or Secure Computing Mode

69. Which of the following keys are the private keys of asymmetric (public) key pairs that are used only once to establish one or more keys ?

A. Public ephemeral key agreement key
B. Asymmetric random number generation keys
C. Symmetric random number generation keys
D. Private Ephemeral Key Agreement Key

D. Private ephemeral key agreement key

70. What does a cryptographic key do within the Internet Layer?

A. It specifies how encrypted data is transferred and to whom.
B. It Specifies How Transferred Information Is Converted Into Cyphertext.

C. It converts it into encrypted language.
D. It is the specialized dataset that is able to decrypt cyphertext.

B. It specifies how transferred information is converted into cyphertext.

71. What is the difference between a worm and virus?

A. A worm does not replicate itself like a virus does, but rather moves from computer to computer
B. A virus infects files, while a worm eats them
C. A worm is a virus created for a very specific purpose
D. Unlike A Virus, A Worm Does Not Need To Attach Itself To A Program To Spread.

D. Unlike a virus, a worm does not need to attach itself to a program to spread.

72. Which of the following represents a cryptographic key that is intended to be used for a long period of time?

A. Private key transport key
B. Public authentication key
C. Public signature verification key
D. Private Static Key Agreement Key

D. Private static key agreement key

73. Which of the following is a VALID ephemeral key?

A. Asymmetric ephemeral random number generation keys
B. Public ephemeral verification key

C. Symmetric ephemeral random number generation keys
D. Public Ephemeral Key Agreement Key

D. Public ephemeral key agreement key

74. Which of the following enables secure and private data exchange/transfer on an unsecure public network ?

A. Public Key Infrastructure
B. Virtual Key Infrastructure
C. Private Key Infrastructure
D. All of the given options are correct

A. Public Key Infrastructure

75. Which of the following keys are used to encrypt other keys using symmetric key algorithms ?

A. Symmetric random number generation keys
B. Asymmetric random number generation keys
C. Symmetric Key Wrapping Key
D. Public signature verification key

C. Symmetric key wrapping key

76. Which of the following keys are used to encrypt other keys using symmetric key algorithms ?

A. Symmetric random number generation keys
B. Asymmetric random number generation keys
C. Symmetric Key Wrapping Key
D. Public signature verification key

C. Symmetric key wrapping key

77. Which of the following is a standalone computer program that pretends to be a well-known program in order to steal confidential data ?

A. Virus
B. Spyware
C. Fraudtool
D. Malware

C. Fraudtool

78. In the sublayer of which of the following does TLS and SSL performs the data encryption of network connections?

A. presentation layer
B. Both session and presentation layer
C. session layer
D. Application Layer

D. application layer

79. Which of the following are the public keys of asymmetric (public) key pairs that are used to encrypt keys using a public key algorithm?

A. Public signature verification key
B. Private signature key
C. Public Key Transport Key
D. Private key transport key

C. Public key transport key

80. Which of the following are the public keys of asymmetric key pairs that are used to encrypt keys using a public key algorithm ?

A. Private signature key
B. Private Key Transport Key
C. Public signature verification key
D. Public authentication key

B. Private key transport key