High School \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

You may write on this contest exam. Record your answers on the scrantron sheet. This is close book, no notes.

On the scrantron sheet enter the following:

LAST NAME:

FIRST NAME

This is a power test. You will have **40 minutes** to complete these 58 **multiple choice questions**. Your score is the number answered correctly. The top 8 students will proceed to the hands-on part of contest in the afternoon.

1 The \_\_\_\_ service addresses the security concerns raised by denial-of –service attacks.

 a. integrity b. availability

 c. event detection d. routing control

2 \_\_\_\_ attacks attempt to alter system resources or affect their operation.

 a. Passive b. Release of message content

 c. Active d. Traffic analysis

3 X.800 defines \_\_\_\_ as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

 a.replay b. integrity

 c. security servicec. authenticity

4 The security goal that generates the equipment for actions of an entity to be traced uniquely to that entity is \_\_\_\_\_\_\_.

 a. accountability b. authenticity

 c. privacy d. integrity

5 The protection of data from unauthorized disclosure is \_\_\_\_\_\_.

 a. nonrepudiation b. data confidentiality

c. access control d. authentication

6 Which of the following can be a type of spyware?

a. A cookie. b. A keystroke logger

c. Both A and B d. Neither A nor B

7 \_\_\_\_ security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information.

 a. Network b. Intranet

 c. Computer d. Internet

8 \_\_\_\_\_\_\_ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

 a. system integrityb. data confidentiality

 b. availability d. privacy

9 ICMP Echo messages are often used in \_\_\_\_\_.

a. IP address scanning b. port scanning

c. Both A and B d. Neither A nor B

10 Sending packets with false IP source addresses is \_\_\_\_\_.

a. a IP address scanning attack b.IP address spoofing

c. a port scanning attack d. None of the above.

11 A(n) \_\_\_\_\_ attack requires a victim host to prepare for many connections, using up resources until the computer can no longer serve legitimate users. (Choose the most specific choice.)

a. DoS b. directly-propagating worm

c. distributed malware d. SYN Flooding

12 \_\_\_\_\_ assures that systems work promptly and service is not denied to authorized users

 a. system integrity b. data confidentiality

 b. availability d. privacy

13 \_\_\_\_\_ is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

 a. Notarization b. Authentication exchange

 c. Routing Control d. Traffic padding

14 The prevention of unauthorized use of a resource is \_\_\_\_\_.

 a. authentication b. access control

 c. data confidentiality c. nonrepudiation

15 Verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

 a. Authenticityb. Confidentiality

 c. Accountability d. Integrity

16 If an attacker breaks into a corporate database and deletes critical files, this is an attack against the \_\_\_\_\_ security goal.

a. integrity b. confidentiality

c. Both A and B d. Neither A nor B

17 A \_\_\_\_\_\_\_\_\_ occur(s) when a single security element failure defeats the overall security of a system.

a. spot failure b. weakest link failure

c. defense in depth departure d. critical failure

18 The key to security being an enabler is \_\_\_\_\_.

a. getting it involved early within the project.

b. having strong corporate policies

c. extensive training

d. adequate spending on security

19 A \_\_\_\_\_\_ takes place when one entity pretends to be a different entity.

 a. modification of message b. replay

 c. passive attack d. masquerade

20 Data integrity is the protection of data from unauthorized disclosure.

 a. True

 b. False

21 The loss of confidentiality is the unauthorized modification or destruction of information

 a. True

 b. False

22 Which of the following is not a compliance regulation?

 a. PCI-DSS b. SOX

 c. PCI-Xc. HIPPA

23 An unauthorized access point operating at 5.0 GHz will be visible to a scan at 2.4 GHz?

 a. True

 b. False

24 Which PCI – DSS requirement mandates that organizations implement a WAF (Web Application Firewall) or conduct application code reviews?

 a. 6.1 b. 3.4

 c. 5.8 d. 6.6

25 What type of product restricts the availability of network resources to endpoint devices based on a defined security policy?

 a. Intrusion detection system (IDS)

b. Intrusion prevention system (IPS)

 c. Network access control (NAC)

d. Data loss prevention (DLP)

26 Change control technology is:

1. A means of preventing false or improper alterations to user-facing services in a data center environment.
2. The monitoring, administration, and tracking of configuration setting to workstations, servers, and transport hardware.
3. A platform for developing change policies and a means to control authorized changes to device configurations, software and operating systems.

27 Which layer(s) of network can Snort, the network IDS, protect against attacks?

 a. Layer 1 and above b. Layer 3 and above

 c. Layer 5 and above d. Layer 7 only

28 Snort can decode all encrypted traffic.

1. True
2. False

29 Which if the following network security tools is used solely as a wireless sniffer that detects 802.xx networks and access points?

 a. Airtrack b. Kismet

 c. Nmap d. Nagios

30 \_\_\_\_\_\_\_ is the use of mathematical operations to protect messages travelling between parties or stored on a computer.

a. Cryptography b. Encryption

c. Authentication d. Confidentiality

31 \_\_\_\_\_\_\_\_ is the security guarantee that people who intercept messages cannot read them.

a. Integrity b. Availability

c. Confidentiality d. Encryption

32 Which of the following controls outbound network access and provides stateful inspection of network traffic?

 a. Router b. Firewall

 c. ACL

33 What kind of security solution monitors for rouge APs and unauthorized devices, maintains policy adherence, monitors for anomalous behavior, and relies on dedicated, distributed hardware sensors that continuously monitor multiband channels and report anomalies?

 a. Overlay WIPS b. Integrated WIDS

 b. Overlays WIDSc. Integrated WIPS

34 When two parties communicate with each other using symmetric key encryption, how many keys are used in total to encrypt and decrypt?

a. 1 b. 2.

c. 4. d. 8.

35 The best way to thwart exhaustive searches by cryptanalysts is \_\_\_\_\_\_\_.

a. to use codes

b. to make the key very long

c. randomize the key thoroughly

d. All of the above.

36 If a key is 43 bits long, how much longer will it take to crack it by exhaustive search if it is extended to 50 bits?

a. 7 times as long. b. 14 times as long.

c. 128 times as long. d. 256 times as long.

37 The Ethernet address of an access point is its \_\_\_\_\_\_\_.

 a. SSID b. BSSID

 c. both A and B d. neither A nor B

38 What is the hash size of SHA-256?

a. 112 bits. b. 128 bits.

c. 160 bits. d. 256 bits.

39 An unauthorized access point is a(n) \_\_\_\_\_\_.

 a. SSID b. BSSID

 c. rogue access point d. evil twin access point

40 Which of the following is a networked application?

 a. the Internet b. the World Wide Web

 c. both A and B d. neither A nor B

41 A device attached to a network is called a \_\_\_\_\_\_.

 a. client b. server

 c. host d. either A or B

42 If two hosts are separated by seven networks, how many packets will there be along the way when a host transmits a packet to another host?

 a. 1 b. 2

 c. 7 d. 14

43 Replay attacks can be thwarted by using \_\_\_\_\_\_\_.

a. time stamps b. sequence numbers

c. All of the above. d. none of the above

44 Which of the following layers governs internet transmission?

 a. data link layer b. transport layer

 b. both A and B c. neither A nor B

45 Which of the following allows an attacker to manipulate filed by using the least significant bit(s) to secretly embed data?

 a. Steganography b. Worm

 c. Trojan horse d. Virus

46 Which of the following types of attacks would allow an attacker to capture HTTP requests and send back a spoofed page?

 a. Teardrop b. TCP/IP hijacking

 c. Phishing d. Replay

47 How should a business test the integrity of its backup data?

1. By conducting another backup
2. By using software to recover deleted files
3. By restoring part of the backup
4. By reviewing the written procedures

48 Which of the following are elements of host hardening?

a. Minimizing applications on the host.

b. Having a good border firewall.

c. Both A and B

d. Neither A nor B

49 Which of the following can best be used to determine the topology of a network and discover unknown devices?

 a. Vulnerability scanner b. NIPS

 c. Protocol analyzer d. Network mapper

50 A(n) \_\_\_\_\_\_ is defined as an attack that comes before fixes are released.

a. exploit b. zero-day attack

c. worm d. anomaly attack

51 When should a technician perform penetration testing?

1. When a technician suspects that weak passwords exist on the network
2. When a technician is trying to guess passwords on a network
3. When a technician has permission from the owner of the network
4. When a technician is war driving and trying to gain access.

52 An administrator has implemented a new SMTP service on a server. A public IP address translates to the internal SMTP server. The administrator notices many sessions to the server, and gets notification that the server’s public IP address is now reported in a spam real-time block list. Which of the following is wrong with the server?

 a. SMTP open relaying is enabled

b. It does not have a spam filter

 c. The amount of sessions needed is limited

 d. The public IP address is limited

53 Which of the following is MOST efficient for encrypting large amounts of data?

 a. Hashing algorithms b. Symmetric key algorithms

 c. Asymmetric key algorithms d. ECC algorithms

54 An attacker types more data in a field than the programmer expected. This is a(n) \_\_\_\_\_ attack.

a. denial-of-service b. directory traversal

c. buffer overflow d. XSS

55 Which of the following BEST describes ARP?

1. Discovering the IP address of a device from the MAC address
2. Discovering the IP address of a device from the DNS name
3. Discovering the MAC address of a device from the IP address
4. Discovering the DNS name of a device from the IP address

56 Which of the following is the most dangerous because it can do more on a computer when it is executed?

a. Active-X b. Java

c. Javascript d. VBscript

57 Which of the following is a reason why a company should disable the SSID broadcast of the wireless access points?

 a. Rogue access points b. Wardriving

 c. Weak encryption d. Session hijacking

58 All of the following provide confidentiality protection as part of the underlying protocol except:

 a. SSL b. SSH

 c. L2TP d. IPSec