1 / 1 point

The smallest building block of a wireless LAN is a \_\_\_\_\_\_\_\_\_\_ which consists of wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium.

Correct answer:

BSS

**Results for question 2.**

2

1 / 1 point

The use of 802.1X cannot prevent rogue access points and other unauthorized devices from becoming insecure backdoors.

True

Correct answer:

False

**Results for question 3.**

3

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ layer is responsible for detecting errors and discarding any frames that contain errors.

Correct answer:

MAC

**Results for question 4.**

4

1 / 1 point

IEEE 802.11 is a standard for wireless LANs.

Correct answer:

True

False

**Results for question 5.**

5

1 / 1 point

The MPDU authentication phase consists of three phases. They are: connect to AS, EAP exchange, and secure \_\_\_\_\_\_\_\_\_ delivery.

Correct answer:

key

**Results for question 6.**

6

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ is the information that is delivered as a unit between MAC users.



MPDU

, Not Selected



BSS

, Not Selected

Correct answer:



MSDU



DS

, Not Selected

**Results for question 7.**

7

1 / 1 point

Forming a hierarchy beginning with a master key from which other keys are derived dynamically and used for a limited period of time, \_\_\_\_\_\_\_\_\_\_ keys are used for communication between a pair of devices typically between a STA and an AP.

Correct answer:

pairwise

**Results for question 8.**

8

1 / 1 point

The pairwise master key is derived from the group key.

True

Correct answer:

False

**Results for question 9.**

9

1 / 1 point

The layer of the IEEE 802 reference model that includes such functions as encoding/decoding of signals and bit transmission/reception is the \_\_\_\_\_\_\_\_\_ .



media access layer

, Not Selected

Correct answer:



physical layer



control layer

, Not Selected



logical link layer

, Not Selected

**Results for question 10.**

10

1 / 1 point

Security policies for mobile devices should assume that any mobile device will not be stolen or accessed by a malicious party.

True

Correct answer:

False

The \_\_\_\_\_\_\_\_\_ transfer encoding is useful when the data consists largely of octets that correspond to printable ASCII characters.

Correct answer:

quoted-printable

**Results for question 2.**

2

1 / 1 point

S/MIME provides the following functions: enveloped data, signed data, clear signed data, and \_\_\_\_\_\_\_\_ and enveloped data.

Correct answer:

signed

**Results for question 3.**

3

1 / 1 point

The key legitimacy field is derived from the collection of signature trust fields in the entry.

Correct answer:

True

False

**Results for question 4.**

4

1 / 1 point

PGP incorporates tools for developing public-key certificate management and a public-key trust model.

Correct answer:

True

False

**Results for question 5.**

5

1 / 1 point

MIME is an extension to the \_\_\_\_\_\_\_\_ framework that is intended to address some of the problems and limitations of the use of SMTP.



RFC 821

, Not Selected



RFC 4871

, Not Selected

Correct answer:



RFC 5322



RFC 3852

, Not Selected

**Results for question 6.**

6

1 / 1 point

Each PGP entity must maintain a file of its own public/private key pairs as well as a file of private keys of correspondents.

True

Correct answer:

False

**Results for question 7.**

7

1 / 1 point

The \_\_\_\_\_\_\_\_\_ type refers to other kinds of data, typically either uninterpreted binary data or information to be processed by a mail-based application.

Correct answer:

application

**Results for question 8.**

8

1 / 1 point

S/MIME cryptographic algorithms use \_\_\_\_\_\_\_\_\_\_ to specify requirement level.



CAN and MUST

, Not Selected



SHOULD and CAN

, Not Selected

Correct answer:



SHOULD and MUST



SHOULD and MIGHT

, Not Selected

**Results for question 9.**

9

1 / 1 point

PGP has a very rigid public-key management scheme.

True

Correct answer:

False

**Results for question 10.**

10

1 / 1 point

The key legitimacy field, the signature trust field, and the owner trust field are each contained in a structure referred to as a \_\_\_\_\_\_\_\_\_\_\_ flag byte.

Correct answer:

trust

\_\_\_\_\_\_\_\_\_ defines a number of techniques for key management.



SKE

, Not Selected



KEP

, Not Selected

Incorrect answer:



IKE

Correct Answer:

SKE



KMP

, Not Selected

**Results for question 2.**

2

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ payload contains either error or status information associated with this SA or this SA negotiation.



Configuration

, Not Selected

Correct answer:



Notify



Nonce

, Not Selected



Encrypted

, Not Selected

**Results for question 3.**

3

1 / 1 point

The key management mechanism that is used to distribute keys is coupled to the authentication and privacy mechanisms only by way of the \_\_\_\_\_\_\_\_\_.



IAB

, Not Selected



SPD

, Not Selected



ESP

, Not Selected

Correct answer:



SPI

**Results for question 4.**

4

1 / 1 point

Both tunnel and transport modes can be accommodated by the encapsulating security payload encryption format.

Correct answer:

True

False

**Results for question 5.**

5

1 / 1 point

The principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level.

Correct answer:

True

False

**Results for question 6.**

6

0 / 1 point

The \_\_\_\_\_\_\_\_\_ facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.

Incorrect answer:



confidentiality

Correct Answer:

authentication



authentication

, Not Selected



key management

, Not Selected



security

, Not Selected

**Results for question 7.**

7

0 / 1 point

The \_\_\_\_\_\_\_\_\_\_ mechanism assures that a received packet was in fact transmitted by the party identified as the source in the packet header and assures that the packet has not been altered in transit.



key management

, Not Selected



confidentiality

, Not Selected

Incorrect answer:



authentication

Correct Answer:

security



security

, Not Selected

**Results for question 8.**

8

1 / 1 point

An end user whose system is equipped with IP security protocols can make a local call to an ISP and gain secure access to a company network.

Correct answer:

True

False

**Results for question 9.**

9

1 / 1 point

Any traffic from the local host to a remote host for purposes of an IKE exchange bypasses the IPsec processing.

Correct answer:

True

False

**Results for question 10.**

10

1 / 1 point

Transport mode provides protection to the entire IP packet.

True

Correct answer:

False

Newer worms are limited to Windows machines.

True

Correct answer:

False

**Results for question 2.**

2

1 / 1 point

\_\_\_\_\_\_\_ is software that collects information from a computer and transmits it to another system.



Exploit

, Not Selected

Correct answer:



Spyware



Trojan horse

, Not Selected



Flooder

, Not Selected

**Results for question 3.**

3

1 / 1 point

During the \_\_\_\_\_\_\_\_\_\_ phase the virus places a copy of itself into other programs or into certain system areas on the disk.



dormant

, Not Selected

Correct answer:



propagation



execution

, Not Selected



triggering

, Not Selected

**Results for question 4.**

4

1 / 1 point

A zombie is a program activated on an infected machine that is activated to launch attacks on other machines.

Correct answer:

True

False

**Results for question 5.**

5

1 / 1 point

To replicate itself, a worm uses some means to access remote systems.

Correct answer:

True

False

**Results for question 6.**

6

1 / 1 point

Viruses often morph to evade detection.

Correct answer:

True

False

**Results for question 7.**

7

1 / 1 point

A\_\_\_\_\_\_\_\_\_\_ is a program that installs other items on a machine that is under attack.

Correct answer:



downloader



logic bomb

, Not Selected



none of the above

, Not Selected



flooder

, Not Selected

**Results for question 8.**

8

1 / 1 point

A polymorphic virus creates copies during replication that are functionally equivalent but have distinctly different bit patterns, in order to defeat programs that scan for viruses.

Correct answer:

True

False

**Results for question 9.**

9

1 / 1 point

There are \_\_\_\_\_\_\_\_\_ generations of antivirus software.

Correct answer:



four



two

, Not Selected



five

, Not Selected



three

, Not Selected

**Results for question 10.**

10

1 / 1 point

Worms cannot spread through shared media, such as USB drives or CD and DVD data disks.

True

Correct answer:

False

Penetration identification is an approach developed to detect deviation from previous usage patterns.

True

Correct answer:

False

**Results for question 2.**

2

1 / 1 point

Traditional hackers usually have specific targets, or at least classes of targets, in mind.

True

Correct answer:

False

**Results for question 3.**

3

1 / 1 point

Software trespass can take the form of a \_\_\_\_\_\_\_\_\_.



worm

, Not Selected



Trojan horse

, Not Selected

Correct answer:



all of the above



virus

, Not Selected

**Results for question 4.**

4

1 / 1 point

A \_\_\_\_\_\_\_\_ is a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.



masquerader

, Not Selected



emissary

, Not Selected

Correct answer:



misfeasor



clandestine user

, Not Selected

**Results for question 5.**

5

1 / 1 point

A \_\_\_\_\_\_\_\_\_ is an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

Correct answer:



masquerader



misfeasor

, Not Selected



sniffer

, Not Selected



clandestine user

, Not Selected

**Results for question 6.**

6

1 / 1 point

\_\_\_\_\_\_\_\_\_ detection focuses on characterizing the past behavior of individual users or related groups of users and then detecting significant deviations.



Threshold

, Not Selected

Correct answer:



Profile-based anomaly



Statistical anomaly

, Not Selected



Action condition

, Not Selected

**Results for question 7.**

7

1 / 1 point

A \_\_\_\_\_\_\_\_ model is based on correlations between two or more variables.



operational

, Not Selected

Correct answer:



multivariate



Markov process

, Not Selected



mean and Standard Deviation

, Not Selected

**Results for question 8.**

8

1 / 1 point

A \_\_\_\_\_\_\_\_ is an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Correct answer:



clandestine user



masquerader

, Not Selected



misfeasor

, Not Selected



mole

, Not Selected

**Results for question 9.**

9

1 / 1 point

A weakness of the IDES approach is its lack of flexibility.

Correct answer:

True

False

**Results for question 10.**

10

1 / 1 point

The simplest statistical test is to measure the \_\_\_\_\_\_\_\_\_ of a parameter over some historical period, which would give a reflection of the average behavior and its variability.

Correct answer:



mean and standard deviation



multivariate

, Not Selected



time series

, Not Selected



Markov process

1

0 / 1 point

What can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet?



SOCKS

, Not Selected

Incorrect answer:



Firewalls

Correct Answer:

VPNs



VPNs

, Not Selected



Proxys

, Not Selected

### Results for question 2.

2

1 / 1 point

Intrusion detection involves detecting unusual patterns of activity or patterns of activity that are known to correlate with intrusions.

Correct answer:

True

False

### Results for question 3.

3

1 / 1 point

The \_\_\_\_\_\_\_\_\_ is used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.

Correct answer:



EAPOL-KEK



TK

, Not Selected



MIC key

, Not Selected



EAPOL-KCK

, Not Selected

### Results for question 4.

4

1 / 1 point

Computed by PGP, a \_\_\_\_\_\_\_\_\_ legitimacy field indicates the extent to which PGP will trust that this is a valid public key for this user; the higher the level of trust, the stronger the binding of this user ID to this key.

Correct answer:

key

### Results for question 5.

5

1 / 1 point

\_\_\_\_\_\_\_\_\_\_ is the primary service used by stations to exchange MPDUs when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS.

Correct answer:

Distribution

### Results for question 6.

6

1 / 1 point

Insider attacks are among the easiest to detect and prevent.

True

Correct answer:

False

### Results for question 7.

7

1 / 1 point

System administrators can stop all attacks and hackers from penetrating their systems by installing software patches.

True

Correct answer:

False

### Results for question 8.

8

1 / 1 point

Authentication must be applied to the entire original IP packet.

True

Correct answer:

False

### Results for question 9.

9

1 / 1 point

The smallest building block of a wireless LAN is a \_\_\_\_\_\_\_\_\_\_ which consists of wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium.

Correct answer:

BSS

### Results for question 10.

10

0 / 1 point

PGP provides compression using the \_\_\_\_\_\_\_\_\_\_ algorithm.

Incorrect answer:

zip

Correct Answer:ZIP

### Results for question 11.

11

0 / 1 point

A specification for cryptographically signing e-mail messages permitting a signing domain to claim responsibility for a message in the mail stream, \_\_\_\_\_\_\_\_\_ allow message recipients to verify the signature by querying the signer's domain directly to retrieve the appropriate public key and thereby confirming that the message was attested to by a party in possession of the private key for the signing domain.

Incorrect answer:

dkim

Correct Answer:DomainKeys Identified Mail, DKIM

### Results for question 12.

12

1 / 1 point

A \_\_\_\_\_\_\_\_\_\_ is any device that contains an IEEE 802.11 conformant MAC and physical layer.



MPU

, Not Selected



MSDU

, Not Selected



service data unit

, Not Selected

Correct answer:



station

### Results for question 13.

13

1 / 1 point

A\_\_\_\_\_\_\_\_\_\_ is a program that installs other items on a machine that is under attack.



flooder

, Not Selected



logic bomb

, Not Selected

Correct answer:



downloader



none of the above

, Not Selected

### Results for question 14.

14

1 / 1 point

\_\_\_\_\_\_\_\_\_ involves counting the number of occurrences of a specific event type over an interval of time.

Correct answer:



Threshold detection



Profile-based system

, Not Selected



Rule-based detection

, Not Selected



Resource usage

, Not Selected

### Results for question 15.

15

1 / 1 point

A virus, although attached to an executable program, cannot do anything that the program is permitted to do.

True

Correct answer:

False

### Results for question 16.

16

1 / 1 point

A zombie is a program activated on an infected machine that is activated to launch attacks on other machines.

Correct answer:

True

False

### Results for question 17.

17

1 / 1 point

Transport mode provides protection to the entire IP packet.

True

Correct answer:

False

### Results for question 18.

18

0 / 1 point

A \_\_\_\_\_\_\_\_\_ signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer, which is then encoded using base64 encoding.

Incorrect answer:

signed

Correct Answer:digital

### Results for question 19.

19

1 / 1 point

\_\_\_\_\_\_\_ can result in pop-up ads or redirection of a browser to a commercial site.



Bots

, Not Selected

Correct answer:



Adware



Kits

, Not Selected



Flooders

, Not Selected

### Results for question 20.

20

1 / 1 point

Which control technique controls how particular services are used, allowing the firewall to filter e-mail to eliminate spam or enable external access to only a portion of the information on a local Web server?

Correct answer:



behavior



service

, Not Selected



user

, Not Selected



direction

, Not Selected

### Results for question 21.

21

1 / 1 point

There are \_\_\_\_\_\_\_\_\_ generations of antivirus software.



three

, Not Selected



five

, Not Selected

Correct answer:



four



two

, Not Selected

### Results for question 22.

22

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ field is used to identify MIME entities uniquely in multiple contexts.



Content-Description

, Not Selected



Content-Transfer- Encoding

, Not Selected



Content-Type

, Not Selected

Correct answer:



Content-ID

### Results for question 23.

23

1 / 1 point

A \_\_\_\_\_\_\_\_ is a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.



masquerader

, Not Selected



emissary

, Not Selected



clandestine user

, Not Selected

Correct answer:



misfeasor

### Results for question 24.

24

1 / 1 point

IP security is a capability that can be added to either current version of the Internet Protocol by means of additional headers.

Correct answer:

True

False

### Results for question 25.

25

1 / 1 point

In which RFC is SOCKS defined as "a framework for client-server applications in both the TCP and UDP domains to conveniently and securely use the services of a network firewall"?



RFC 1046

, Not Selected



RFC 1935

, Not Selected

Correct answer:



RFC 1928



RFC 1024

, Not Selected

### Results for question 26.

26

1 / 1 point

To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using \_\_\_\_\_\_\_\_\_-64 conversion.

Correct answer:

radix

### Results for question 27.

27

1 / 1 point

An individual SA can implement both the AH and the ESP protocol.

True

Correct answer:

False

### Results for question 28.

28

1 / 1 point

\_\_\_\_\_\_\_\_\_ consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication. The current specification is RFC 4303.



SPI

, Not Selected



IPsec

, Not Selected



ISA

, Not Selected

Correct answer:



ESP

### Results for question 29.

29

1 / 1 point

\_\_\_\_\_\_\_ is software that collects information from a computer and transmits it to another system.

Correct answer:



Spyware



Exploit

, Not Selected



Flooder

, Not Selected



Trojan horse

, Not Selected

### Results for question 30.

30

1 / 1 point

In a \_\_\_\_\_\_\_\_ attack the attacker is able to implant zombie software on a number of sites distributed throughout the Internet.



DoS

, Not Selected



bot

, Not Selected

Correct answer:



direct DDoS



reflector DDoS

, Not Selected

### Results for question 31.

31

1 / 1 point

Usually, a downloader is sent in an e-mail.

Correct answer:

True

False

### Results for question 32.

32

1 / 1 point

To certify interoperability for 802.11b products, an industry consortium named the \_\_\_\_\_\_\_\_\_\_ was formed.

Correct answer:

WECA

### Results for question 33.

33

1 / 1 point

The principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level.

Correct answer:

True

False

### Results for question 34.

34

1 / 1 point

In simple terms, the wireless environment consists of three components that provide a point of attack: the endpoint, the \_\_\_\_\_\_\_\_\_\_\_\_\_\_ medium, and the access point.

Correct answer:

wireless

### Results for question 35.

35

1 / 1 point

Due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations.

Correct answer:

True

False

### Results for question 36.

36

1 / 1 point

Malicious software constitutes one of the most significant categories of threats to computer systems.

Correct answer:

True

False

### Results for question 37.

37

1 / 1 point

PGP incorporates tools for developing public-key certificate management and a public-key trust model.

Correct answer:

True

False

### Results for question 38.

38

1 / 1 point

Propagation mechanisms include system corruption, bots, phishing, spyware, and rootkits.

True

Correct answer:

False

### Results for question 39.

39

1 / 1 point

MIME is an extension to the \_\_\_\_\_\_\_\_ framework that is intended to address some of the problems and limitations of the use of SMTP.



RFC 3852

, Not Selected



RFC 821

, Not Selected



RFC 4871

, Not Selected

Correct answer:



RFC 5322

### Results for question 40.

40

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ mechanism assures that a received packet was in fact transmitted by the party identified as the source in the packet header and assures that the packet has not been altered in transit.



authentication

, Not Selected



key management

, Not Selected



confidentiality

, Not Selected

Correct answer:



security

### Results for question 41.

41

1 / 1 point

A firewall may be designed to operate as a filter at the level of IP packets or may operate at a higher protocol layer.

Correct answer:

True

False

### Results for question 42.

42

1 / 1 point

The specification of a protocol along with the chosen key length is known as a \_\_\_\_\_\_\_\_\_\_ .

Correct answer:



cipher suite



extended service

, Not Selected



RSN

, Not Selected



distribution system

, Not Selected

### Results for question 43.

43

0 / 1 point

A firewall may not act as a packet filter.

True

Incorrect answer:

False

Correct Answer:True

### Results for question 44.

44

1 / 1 point

What is an important aspect of a distributed firewall configuration?



network frame locking

, Not Selected



configuration alerting

, Not Selected



change control

, Not Selected

Correct answer:



security monitoring

### Results for question 45.

45

1 / 1 point

The ID determines the privileges accorded to the user.

Correct answer:

True

False

### Results for question 46.

46

1 / 1 point

What configuration is common for large businesses and government organizations and is required for Australian government use?



Single bastion inline

, Not Selected



Single bastion T

, Not Selected



Double bastion inline

, Not Selected

Correct answer:



Double bastion T

### Results for question 47.

47

1 / 1 point

An operation such as login, read, perform, I/O, or execute that is performed by the subject on or with an object is the \_\_\_\_\_\_\_\_\_ audit record field.



object

, Not Selected

Correct answer:



action



resource-usage

, Not Selected



subject

, Not Selected

### Results for question 48.

48

1 / 1 point

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.

Correct answer:

True

False

### Results for question 49.

49

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ payload contains either error or status information associated with this SA or this SA negotiation.



Encrypted

, Not Selected



Configuration

, Not Selected



Nonce

, Not Selected

Correct answer:



Notify

### Results for question 50.

50

1 / 1 point

The \_\_\_\_\_\_\_\_\_ payload allows peers to identify packet flows for processing by IPsec services.



Configuration

, Not Selected



Vendor ID

, Not Selected



Extensible Authentication Protocol

, Not Selected

Correct answer:



Traffic Selector

### Results for question 51.

51

1 / 1 point

The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption.

Correct answer:

True

False

### Results for question 52.

52

1 / 1 point

The most promising approach to improved password security is \_\_\_\_\_\_\_\_\_\_.



a reactive password checking strategy

, Not Selected



user education

, Not Selected



computer-generated passwords

, Not Selected

Correct answer:



a proactive password checker

### Results for question 53.

53

0 / 1 point

Packet filters tend to be more secure than application-level gateways.

True

Incorrect answer:

False

Correct Answer:True

### Results for question 54.

54

1 / 1 point

Unauthorized intrusion into a computer system or network is one of the most serious threats to computer security.

Correct answer:

True

False

### Results for question 55.

55

1 / 1 point

\_\_\_\_\_\_\_\_\_\_ is an Internet standard approach to e-mail security that incorporates the same functionality as PGP.



DKIM

, Not Selected



MIME

, Not Selected



HTTPS

, Not Selected

Correct answer:



S/MIME

### Results for question 56.

56

1 / 1 point

Software trespass can take the form of a \_\_\_\_\_\_\_\_\_.



virus

, Not Selected



Trojan horse

, Not Selected



worm

, Not Selected

Correct answer:



all of the above

### Results for question 57.

57

1 / 1 point

S/MIME provides the following functions: enveloped data, signed data, clear signed data, and \_\_\_\_\_\_\_\_ and enveloped data.

Correct answer:

signed

### Results for question 58.

58

1 / 1 point

A \_\_\_\_\_\_\_\_\_ is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.



SAD

, Not Selected

Correct answer:



SA



SPD

, Not Selected



SPI

, Not Selected

### Results for question 59.

59

1 / 1 point

Handheld PDAs pose a security risk in terms of both eavesdropping and spoofing.

Correct answer:

True

False

### Results for question 60.

60

0 / 1 point

An \_\_\_\_\_\_\_\_\_\_ is a set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.

Incorrect answer:

Extended service set

Correct Answer:extended service set, ESS