1. Which wireless mode involves two laptops connecting directly to one another?  
B. Ad hoc mode

2. Which of the following wireless standards does not fall into the Wi-Fi standard?  
D. 802.11a

3. Which wireless standard runs at 54 Mbps at the 2.4-GHz frequency?  
C. 802.11g

4. Which wireless standard can reach transfer rates of up to 600 Mbps?  
A. 802.11n

5. Which wireless security protocol changes the key using TKIP?  
B. WPA

6. Which wireless security protocol uses CCMP and AES to perform the encryption of the  
communication?  
D. WPA2  
  
7. Which of the following is the name you assign to your wireless network?  
B. Service Set Identifier (SSID)

8. What should you do with the wireless router to help hide the wireless network from  
unauthorized users?  
C. Disable SSID broadcasting.

9. You wish to encrypt traffic between the wireless client and the access point, but you don’t have a  
wireless router that supports WPA or WPA2. What would you do to secure the traffic?  
D. Use WEP on both the client and the router.

10. Derek is performing a wireless site survey and has found a wireless router connected to the  
network. Looking out the window next to where he found the wireless router, Derek also notices  
some strange markings on the building across the street. What is the term for these markings?  
D. War chalking

11. Sean, a senior security officer for your company, has been monitoring wireless activity for some  
time and suspects that an attacker has spoofed the MAC address on their network card to gain  
access to the network. What wireless security feature has been compromised in this example?  
A. MAC filtering

12. Sue is responsible for configuring the wireless network for Jetstream, Inc. Management has  
expressed great concern about wireless security and would like to ensure that anyone outside the  
building cannot connect to the wireless network. What should Sue do?  
A. Configure MAC filtering.

13. Jeff is a junior security officer for Company XYZ and is currently responsible for the security  
of the company’s wireless network. Jeff is working on configuring the wireless encryption and  
wants to use the most secure encryption option with a RADIUS server for authentication. Which  
encryption option should he use?  
E. WPA2 Enterprise

14. Dan, a security engineer for your company, has recently limited which devices can connect to  
each port on the switch by MAC address. Which of the following wireless attack methods is  
Dan mitigating?

C. Rogue access point

15. What is the first thing you should change on the wireless router when it is powered on?  
B. The admin password

16. You have just purchased a wireless router but do not intend to have any wireless clients for the  
first six months. What should you do to help secure the router?  
D. Disable the wireless features.

17. What program could be used to do a survey of your area and discover wireless networks?  
(Select two.)  
C. Cain & Abel  
E. Kismet  
  
18. What is the transfer rate of Bluetooth?  
B. 1 Mbps

19. What type of wireless vulnerability involves exploiting a Bluetooth device and copying data off the  
device?  
C. Bluesnarfing

20. Tom has recently received a number of unwanted advertisements on his mobile device. What type  
of attack has occurred?  
A. Bluejacking

21.

|  |  |
| --- | --- |
| Used to control which devices can connect | MAC Filtering |
| Wireless encryption using a password | WPA2 Personal |
| Used to ensure someone is close to the wireless router in order to connect | Power Level |
| Used to hide the wireless network | Disable SSID Broadcasting |
| Wireless encryption using a RADIUS server for authentication | WPA2 Enterprise |