## QUESTIONS

1. A vendor is alerted of a newly discovered flaw in its software that presents a major vulnerability to systems. While working to prepare a fix action, the vendor releases a notice alerting the community of the discovered flaw and providing best practices to follow until the patch is available. Which of the following best describes the discovered flaw?

   A. Input validation flaw

   B. Shrink-wrap vulnerability

   C. Insider vulnerability

   D. Zero-day

2. A security professional applies encryption methods to communication channels. Which security control role is she attempting to meet?

   A. Preventive

   B. Detective

   C. Defensive

   D. Corrective

3. Which of the following comes after scanning in the CEH methodology for testing a system?

   A. Gaining access

   B. Reconnaissance

   C. Maintaining access

   D. Covering tracks

4. An organization allows the data owner to set security permissions on an object. Which access control mechanism is in place?

   A. Mandatory access control

   B. Role-based access control

   C. Discretionary access control

   D. Authorized access control

5. Which of the following is true regarding MX records?

   A. MX records require an accompanying CNAME record.

   B. MX records point to name servers.

   C. MX record priority increases as the preference number decreases.

   D. MX record entries are required for every namespace.

6. From the partial e-mail header provided, which of the following represents the true originator of the e-mail message?

```
...
Return-path: <SOMEONE@anybiz.com>
Delivery-date: Wed, 13 Apr 2011 00:31:13 +0200
Received: from mailexchanger.anotherbiz.com([185.213.4.77])
by mailserver.anotherbiz.com running ExIM with esmtp
id xxxxxx-xxxxxx-xxx; Wed, 13 Apr 2011 01:39:23 +0200
Received: from mailserver.anybiz.com ([177.190.50.254] helo=mailserver
.anybiz.com)
by mailexchanger.anotherbiz.com with esmtp id xxxxxx-xxxxxx-xx
for USERJOE@anotherbiz.com; Wed, 13 Apr 2011 01:39:23 +0200
Received: from SOMEONEComputer [229.88.53.154] (helo=[SOMEONEcomputer])
by mailserver.anybiz.com with esmtpa (Exim x.xx)
(envelope-from <SOMEONE@anybiz.com) id xxxxx-xxxxxx-xxxx
for USERJOE@anotherbiz.com; Tue, 12 Apr 2011 20:36:08 -0100
Message-ID: <xxxxxxxx.xxxxxxxx@anybiz.com>
Date: Tue, 12 Apr 2011 20:36:01 -0100
X-Mailer: Mail Client
From: SOMEONE Name <SOMEONE@anybiz.com>
To: USERJOE Name <USERJOE@anotherbiz.com>
Subject: Something to consider
...
```

A. The originator is 185.213.4.77.

B. The originator is 177.190.50.254.

C. The originator is 229.88.53.154.

D. The e-mail header does not show this information.

7. What is the primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.

B. CSIRT provides computer security surveillance to governments, supplying important intelligence information on individuals traveling abroad.

C. CSIRT provides pen testing services to individuals and multinational corporations.

D. CSIRT provides vulnerability assessment services to law enforcement agencies.

8. Which Google operator is the best choice in searching for a particular string in the website's title?

A. intext:

B. inurl:

C. site:

D. intitle:

9. An ethical hacker begins by visiting the target's website and then peruses social networking sites and job boards looking for information and building a profile on the organization. Which of the following best describes this effort?

   A. Active footprinting

   B. Passive footprinting

   C. Internet footprinting

   D. Sniffing

10. Which of the following methods correctly performs banner grabbing with Telnet on a Windows system?

    A. telnet <IPAddress> 80

    B. telnet 80 <IPAddress>

    C. telnet <IPAddress> 80 -u

    D. telnet 80 <IPAddress> -u

11. You are examining results of a SYN scan. A port returns a RST/ACK. What does this mean?

    A. The port is open.

    B. The port is closed.

    C. The port is filtered.

    D. Information about this port cannot be gathered.

12. Which TCP flag instructs the recipient to ignore buffering constraints and immediately send all data?

    A. URG

    B. PSH

    C. RST

    D. BUF

13. You want to run a reliable scan but remain as stealthy as possible. Which of the following Nmap commands accomplishes your goal best?

    A. nmap –sN targetIPaddress

    B. nmap –sO targetIPaddress

    C. nmap –sS targetIPaddress

    D. nmap –sT targetIPaddress

14. As your IDLE scan moves along, you notice that fragment identification numbers gleaned from the zombie machine are incrementing randomly. What does this mean?

    A. Your IDLE scan results will not be useful to you.

    B. The zombie system is a honeypot.

    C. There is a misbehaving firewall between you and the zombie machine.

    D. This is an expected result during an IDLE scan.

15. What step immediately follows banner grabbing in EC-Council's scanning methodology?

    A. Check for live systems

    B. Check for open ports

    C. Scan for vulnerabilities

    D. Draw network diagrams

    E. Prepare proxies

16. Which of the following correctly describes the TCP three-way handshake?

    A. SYN, ACK, SYN/ACK

    B. SYN, SYN/ACK, ACK

    C. ACK, SYN, ACK/SYN

    D. ACK, ACK/SYN, SYN

17. The loopback address represents the local host and in IPv4 was represented by 127.0.0.1. What is the loopback address in IPv6?

    A. fe80::/10

    B. fc00::/7

    C. fec0::/10

    D. ::1

18. Angie captures traffic using Wireshark. Which filter should she apply to see only packets sent from 220.99.88.77?

    A. ip = 220.99.88.77

    B. ip.src == 220.99.88.77

    C. ip.equals 220.99.88.77

    D. ip.addr == 220.99.88.77

19. Given the following Wireshark filter, what is the attacker attempting to view?

```
((tcp.flags == 0x02) || (tcp.flags == 0x12) ) || ((tcp.flags == 0x10) &&
(tcp.ack==1) && (tcp.len==0) )
```

A. SYN, SYN/ACK, ACK

B. SYN, FIN, URG, and PSH

C. ACK, ACK, SYN, URG

D. SYN/ACK only

20. An ACK scan from an external location produces responses from machines inside the target network. Which of the following best describes the circumstances?

A. The IDS is not functioning for the DMZ subnet.

B. The systems are Unix machines.

C. The systems are Windows based.

D. The external firewall is not performing stateful inspection.

21. A pen tester connects a laptop to a switch port and enables promiscuous mode on the NIC. He then turns on Wireshark and leaves for the day, hoping to catch interesting traffic over the next few hours. Which of the following is true regarding this scenario? (Choose all that apply.)

A. The packet capture will provide the MAC addresses of other machines connected to the switch.

B. The packet capture will provide only the MAC addresses of the laptop and the default gateway.

C. The packet capture will display all traffic intended for the laptop.

D. The packet capture will display all traffic intended for the default gateway.

22. Which of the following protocols are considered susceptible to sniffing? (Choose all that apply.)

A. FTP

B. IMAP

C. Telnet

D. POP

E. SMTP

F. SSH

23. What does the following Snort rule accomplish?

```
alert tcp any any -> any 23(msg: "Telnet Connection Attempt")?
```

A. The rule logs any Telnet attempt over port 23 to any internal client.

B. The rule logs any Telnet attempt over port 23 leaving the internal network.

C. The rule alerts the monitor of any Telnet attempt to an internal client.

D. The rule alerts the monitor of any Telnet attempt leaving the internal network.

24. Where is the SAM file found on a Windows 7 machine?

A. C:\windows\config

B. C:\windows\system32

C. C:\windows\system32\etc

D. C:\windows\system32\config

25. Which of the following commands would be useful in adjusting settings on the built-in firewall on a Windows machine?

A. The netstat command

B. The netsh command

C. The sc command

D. The ntfw command

26. Which password cracking method usually takes the most time and uses the most resources?

A. Hybrid

B. Dictionary

C. Brute force

D. Bot-net

27. Which SID indicates the true administrator account on the Windows machine?

A. S-1-5-31-1045337334-12924807993-5683276715-1500

B. S-1-5-31-1045337334-12924807993-5683276715-1001

C. S-1-5-31-1045337334-12924807993-5683276715-501

D. S-1-5-31-1045337334-12924807993-5683276715-500

28. Which of the following keyloggers provides the greatest risk because it cannot be detected by antivirus software?

A. Polymorphic

B. Heuristic

C. Hardware

D. Software

29. Which of the following is true regarding LM hashes?

   A. If the left side of the hash begins with 1404EE, the password is less than eight characters.

   B. If the right side of the hash ends with 1404EE, the password is less than eight characters.

   C. There is no way to tell whether passwords are less than eight characters because hashes are not reversible.

   D. There is no way to tell whether passwords are less than eight characters because each hash is always 32 characters long.

30. Which of the following is considered the most secure password?

   A. Ireallyhateshortpasswords

   B. Apassword123

   C. CEHPassw)rd

   D. Ap@ssw0rd123

31. The < character opens an HTML tag, while the > character closes it. In some web forms, input validation may deny these characters to protect against XSS. Which of the following represents the HTML entities used in place of these characters? (Choose two.)

   A. &lt;

   B. &gt;

   C. &amp;

   D. &reg;

   E. &nbsp;

32. An attacker discovers a form on a target organization's website. He interjects some simple JavaScript into one of the form fields, instead of the username. Which attack is he carrying out?

   A. XSS

   B. SQL injection

   C. Buffer overflow

   D. Brute force

33. An attackers enters the following into a web form: ***' or 1=1*** --. Which attack is being attempted?

   A. XSS

   B. Brute force

C. Parameter manipulation

D. SQL injection

34. You are discussing different web application attacks and mitigations against them. Which of the following is a proper mitigation against cross-site scripting attacks?

A. Configure strong passwords.

B. Ensure the web server is behind a firewall.

C. Ensure the web server is behind an IDS.

D. Perform input validation.

35. Which of the following describes a primary advantage for using Digest authentication over Basic authentication?

A. Digest authentication never sends a password in clear text over the network.

B. Digest authentication uses multifactor authentication.

C. In Digest authentication, the password is sent in clear text over the network but is never reused.

D. In Digest authentication, Kerberos is used to encrypt the password.

36. In HTTP, passwords can be passed in a variety of means—many of them insecure. Which of the following methods is used to encode passwords within HTTP basic access authentication?

A. MD5

B. TDM

C. FDM

D. Base64

E. DES

37. After a recent attack, log files are reviewed by the IR team to determine attack scope, success or failure, and lessons learned. Concerning the following entry:

```
SELECT username, password FROM users;
```

Which of the following best describes the result of this command query?

A. The command deletes username and password fields from a table named *users*.

B. The command adds username and password fields to a table named *users*.

C. The command displays the contents of the username and password fields stored in the table named *users*.

D. The command will not produce any results.

38. An attacker performs reconnaissance and learns the organization's SSID. He places an access point inside a closet, which tricks normal users into connecting, and begins redirecting them to malicious sites. Which of the following categorizes this attack?

A. Replay attack

B. Evil twin attack

C. Closet AP attack

D. WEP nap attack

39. During a pen test, the team lead decides to attempt intrusion using the organization's BlackBerry enterprise. Which tool is used in the blackjacking attempt?

A. Aircrack

B. Kismet

C. BBProxy

D. PrismStumbler

40. Which of the following is a passive wireless discovery tool?

A. NetStumbler

B. Aircrack

C. Kismet

D. Netsniff

41. Which of the following is not true regarding SSIDs?

A. They are used to identify networks.

B. They are used to encrypt traffic on networks.

C. They can be a maximum of 32 characters.

D. Even when not broadcast, SSIDs are easily discovered.

42. Which of the following are true regarding wireless security? (Choose all that apply.)

A. WPA-2 is the best available encryption security for the system.

B. WEP is the best encryption security for the system.

C. Regardless of encryption, turning off SSID broadcast protects the system.

D. SSIDs do not provide any effective security measures for a wireless network.

43. Which command displays all connections and listening ports in numerical form?

A. netstat –an

B. netstat –a localhost –n

C. netstat –r

D. netstat –s

44. Which of the following is true regarding session hijacking?

A. The session must be hijacked before authentication.

B. The session is hijacked after authentication.

C. Strong authentication measures eliminate session hijacking concerns.

D. Session hijacking cannot be carried out against Windows 7 machines.

45. Which virus type overwrites otherwise empty areas within a file?

A. Polymorphic

B. Cavity

C. Macro

D. Boot sector

46. Which of the following is not a field within an X.509 standard certificate?

A. Version

B. Algorithm ID

C. Private key

D. Public key

E. Key usage

47. Which of the following is a common registry location for malware insertion?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce

E. All the above

48. Which of the following is a symmetric cryptographic standard?

A. AES

B. PKI

C. RSA

D. 3DES

49. Which of the following could be a potentially effective countermeasure against social engineering?

    A. User education and training

    B. Strong security policy and procedure

    C. Clear operational guidelines

    D. Proper classification of information and individuals' access to that information

    E. All of the above

50. Which of the following represents the highest risk to an organization?

    A. Black hat

    B. Gray hat

    C. White hat

    D. Disgruntled employee

51. Jill receives an e-mail that appears legitimate and clicks the included link. She is taken to a malicious website that steals her login credentials. Which of the following best describes this attack?

    A. Phishing

    B. Javelin

    C. Wiresharking

    D. Bait and switch

52. Angie waits by a side door entrance and follows a group of employees inside. She has no visible badge of any kind. Which of the following best describes this action?

    A. Tailgating

    B. Piggybacking

    C. Surfing

    D. Reverse SE

53. Bill is asked to perform an assessment but is provided with no knowledge of the system other than the name of the organization. Which of the following best describes the test he will be performing?

    A. White box

    B. Gray box

    C. Black box

    D. None of the above

54. OWASP provides a testing methodology. Which of the following is provided to assist in securing web applications?

  A. COBIT

  B. A list of potential security flaws and mitigations to address them

  C. Web application patches

  D. Federally recognized security accreditation

55. Joe is an IT security consultant, specializing in social engineering. Joe has been given authority to perform any and all tests necessary to audit the company's network security, and no employees know about his efforts. After obtaining a list of employees through company website contact pages, Joe befriends an employee of the company. Soon thereafter, Joe steals the employee's access badge and uses it to gain unauthorized access to the organization offices. What type of insider threat would Joe be considered?

  A. Insider affiliate

  B. Outside affiliate

  C. Inside associate

  D. Pure insider