Mock Exam 1

1. You are an administrator for a college that has 10 intranet web servers, and you need to install an X509 certificate so that they can support HTTPS. You need to use the solution that is the most cost-effective. Which of the following will you use for the certificates?

   a. Wildcard

   b. Domain

   c. Self-signed

   d. SAN

2. Which of the following threat intelligence sources is likely to provide much more accurate data?

   a. OSINT

   b. Public/private information sharing centers

   c. Closed/proprietary

   d. Threat maps

3. A cybersecurity administrator wants to add comments to a log file that they are monitoring. Which tool is best for this?

   a. Nmap

   b. Head

   c. Logger

   d. Tail

4. A cybersecurity team has been attacked by a group of hackers from the internet. The cybersecurity team wishes to find all of the email addresses of this group. Which tool would be the best for this?

   a. Dimitri

   b. The harvester

   c. Curl

   d. Logger

5. Which of the following tools can be used for banner grabbing?

   a. Curl

   b. Telnet

   c. Nmap

   d. netcat (`nc`)

6. A cybersecurity analyst has just finished reading the monthly release from a security advisory. They have now started searching the log files on all of the database servers. What task are they completing?

   a. Log analysis

   b. Risk mitigation

   c. Security administration

   d. Threat hunting

7. A vendor has stopped selling a product, but they still sell a limited number of replacement parts. Which of the following describes the product?

   a. Legacy

   b. End of life

   c. End of service

   d. Retired

8. A security administrator needs to implement secure authentication between two car manufacturers who are going to work on a joint venture. Which of the following should they adopt?

   a. Kerberos

   b. OAuth

   c. Single sign-on

   d. SAML

9. Which of the following regulations deals with credit card purchases and financial transactions?

   a. GDPR

   b. HIPAA

   c. PCI DSS

   d. All of the above

10. Which of the following can be used to protect data stored on mobile telephones? Select two.

    a. TLS

    b. SSL

    c. FDE

    d. Remote wipe

    e. Screen locks

    f. Cable locks

11. You are the security administrator for the British secret service. What type of access method will you use for secret and top-secret data?

    a. You will use DAC, with the owner of the data giving access.

    b. You will use MAC, with the custodian of the data giving access.

    c. You will use DAC, with the security administrator giving access.

    d. You will use MAC, with the security administrator giving access.

12. John goes to a sports website and gets the following error: **THIS WEBSITE CANNOT BE TRUSTED**. What two actions does the website administrator need to take to resolve this error?

    a. Ask the key escrow to store his private key.

    b. Ensure that the website uses a valid SAN certificate.

    c. Update the root certificate into the client computer's trusted root certificate authority's store.

    d. Verify whether the certificate on the server has expired.

13. You are the security administrator for a large multinational company and you have read a security bulletin that mentioned that the CRL for certificate validation has many security flaws. Which of the following will you implement?

    a. Certificate stapling

    b. Certificate pinning

    c. OCSP

    d. Key escrow

14. A security administrator discovers that an attacker used a compromised host as a platform for launching attacks deep in a company's network. What terminology best describes the use of the compromised host?

    a. Brute force

    b. Active reconnaissance

    c. Pivoting

    d. Passing point

15. A security administrator has noticed the following output collected by the SIEM system: Pinging Server 1 with 45,000 bytes of data:

```
Reply from 192.0.0.1: bytes=45000 time<1ms TTL=128
Reply from 192.0.0.1: bytes=45000 time<1ms TTL=128
Reply from 192.0.0.1: bytes=45000 time<1ms TTL=128
Reply from 192.0.0.1: bytes=45000 time<1ms TTL=128
```

What type of attack has been detected?

a. Integer overflow

b. Buffer overflow

c. XSS

d. SQL injection

16. During automation, which of the following is used to identify failures and helps detect security incidents. Select the best option.

a. Continuous validation

b. Continuous monitoring

c. Continuous integration

d. Continuous development

e. Automated courses of action

f. Continuous development

17. A large company is looking to purchase a cybersecurity company and would like a very detailed report about the security controls, in particular, the handling of data, ensuring it is confidential. What reports would the large company want to read so that it can make a good decision on whether to buy or not?

a. SOC 4 reports

b. SOC 1 reports

c. SOC 2 reports

d. SOC 3 reports

18. You are a security administrator for a large multinational company, and you have recently removed data from a data field, and it is now being held by a payment provider. What have you just implemented?

    a. Tokenization

    b. Obfuscation

    c. Data masking

    d. Encryption

19. The network administrator is going to set up a VPN that ensures that both the header and payload are encrypted. What did the security analyst recommend?

    a. IPSec in tunnel mode

    b. IPSec in split-tunnel mode

    c. IPSec in transport mode

    d. IPSec in full-tunnel mode

20. You are the CEO of a large multinational company and you are looking to move to the cloud. Which of the following will help you assess the overall risk of a cloud provider?

    a. CSA reference architecture

    b. CSA CCM

    c. NIST

    d. CASB

21. The security administrator is going to open a risk register for the company. What will be recorded in the risk register?

    a. Risk mitigation techniques

    b. Risk descriptions, the owner, and the mitigation strategies

    c. The annual risk audit report

    d. All of the above

22. An auditor made a recommendation in an annual audit last year that an embedded device be patched immediately. A year later, a second audit made the same recommendation and noted the fact that the outcomes from the last audit had not been adhered to. What is the reason that the patching has not been carried out? Select the most likely reason.

    a. The audit recommendation has been ignored.

    b. The company disagreed with the audit recommendation.

    c. The vendor is not producing any more patches as it is end of life.

    d. There is no interface for patching.

23. The IT manager is designing a BIA plan and is calculating the amount of time in a disaster recovery system that the company can operate without its data. What are they measuring?

    a. RTO

    b. A single point of failure

    c. SLA

    d. RPO

    e. MTTR

24. A security administrator wants to know which services are running on their mail server. What two tools are they most likely to use?

    a. NIDS

    b. Nmap

    c. ipconfig

    d. netstat

    e. Nbtstat

    f. Autopsy

25. Company A is due to upgrade all of its IT systems and has been investigating moving to the cloud as there is no capital expenditure since the CSP provides the hardware. Company A would still like to control the IT systems in the cloud. Which cloud model would best serve Company A's needs?

    a. Software as a Service (SaaS)

    b. Infrastructure as a Service (IaaS)

    c. Monitoring as a Service (MaaS)

    d. Platform as a Service (PaaS)

26. Which of the following RAID systems uses four disks that give you the best resiliency?

    a. RAID 0

    b. RAID 1

    c. RAID 2

    d. RAID 5

    e. RAID 6

27. A data owner is responsible for the classification of data and deciding who can access the data. Who is responsible for ensuring that the collection of data is legal, that the storage is legal, and that compliance has been carried out at all times? Select the best choice.

    a. Data custodian

    b. Privacy officer

    c. Data controller

    d. Data steward

28. You are a security administrator, and the IT director has tasked you with collecting the volatile memory on server 1 as it is currently experiencing a cyber-attack. Which of the following are the two best forms of volatile memory to collect?

    a. Secure boot

    b. Swap/page file

    c. USB flash drive

    d. ROM

    e. RAM

29. At what stage of the SDLC are computer systems no longer supported by the original vendor?

    a. Sandboxing

    b. End-of-life systems

    c. Resource exhaustion

    d. System sprawl

30. Company A has just developed a bespoke system for booking airline tickets. What is it called if a freelance coding specialist tests it for security flaws?

    a. Code review

    b. Static code review

    c. Regression testing

    d. Dynamic code review

31. You are the security administrator for a company that has just replaced two file servers. Which of the following is the best solution for disposing of hard drives that used to store top-secret data?

    a. Hashing

    b. Degaussing

    c. Low-level formatting

    d. Shredding

32. You are the security administrator for an airline company whose systems suffered a loss of availability last month. Which of the following attacks would most likely affect the availability of your IT systems?

    a. Spear phishing

    b. Replay

    c. MITM

    d. DoS

33. Company A has suffered a DDoS attack, and the company has decided that its RPO should be set at 4 hours. The directors are holding a board meeting to discuss the progress that is being made. During this meeting, the IT manager has mentioned the RTO, and the CEO looks confused. How can you explain the meaning of RTO to the CEO?

    a. Acceptable downtime

    b. Return to operational state

    c. Measure of reliability

    d. Average time to repair

34. Which of the following will prevent an SSL man-in-the-middle attack?

    a. Certificate pinning

    b. Input validation

    c. Certificate stapling

    d. Kerberos

35. The security team has identified an unknown vulnerability and isolated it. What technique is best for investigating and testing it?

    a. Steganography

    b. Fuzzing

    c. Sandboxing

    d. Containerization

36. You are the security administrator for your company, and the IT manager has asked you to brief them on XML authentication methods. Which of the following should you tell them uses XML-based authentication? Select all that apply.

    a. TOTP

    b. Federation Services

    c. Smart card

    d. SSO

    e. SOAP

    f. SAML

37. An attacker tries to target a high-level executive but has to leave a voicemail as they did not answer the telephone. What was the intended attack, and what attack was eventually used? Select all that apply.

    a. Whaling

    b. Vishing

    c. Phishing

    d. Spear phishing

38. The auditor has been investigating money being stolen from a charity, and they have discovered that the finance assistant has been embezzling money, as they were the only person who dealt with finance, receiving donations and paying all of the bills. Which of the following is the best option that the auditor could recommend to reduce the risk of this happening again?

    a. Hashing

    b. Job rotation

    c. Separation of duties

    d. Mandatory vacations

    e. Encryption

39. James has raised a ticket with the IT help desk. He had been tampering with the settings on his computer and he can no longer access the internet. The help desk technicians have checked the configuration on his desktop and the settings are the same as everyone else's. Suddenly, three other people have also reported that they also cannot connect to the internet. Which network device should be checked first?

    a. Switch

    b. Router

    c. Hub

    d. Repeater

40. Your company is opening up a new data center in Galway, Ireland. A server farm has been installed there and now a construction company has come in to put a 6-foot mantrap at the entrance. What are the two main reasons why this mantrap will be installed?

    a. To prevent theft

    b. To prevent tailgating

    c. To prevent unauthorized personnel from gaining access to the data center

    d. To allow faster access to the facility

41. What type of trust model do cloud providers use?

    a. Full trust

    b. Bridge trust

    c. Web of trust

    d. Zero trust

42. What two factors does a forensic examiner need when they are going to investigate a cloud-based attack. Choose two.

    a. Right-to-audit clause

    b. Access token

    c. Volatile evidence

    d. Search warrant

43. An auditor has just finished a risk assessment of the company, and they have recommended that we need to mitigate some of our risks. Which of the following are examples of risk mitigation?

    a. Turning off host-based firewalls on laptops

    b. Installing antivirus software on a new laptop

    c. Insuring your car against fire and theft

    d. Outsourcing your IT to another company

    e. Deciding not to jump into the Grand Canyon

44. You work for a very large company that has undergone an audit and the auditor has been looking at the amount of data that you hold. The auditor made recommendations about reducing data retention times for PII and sensitive data. Which of the following concepts is the auditor looking at?

    a. Tokenization

    b. Data retention policy

    c. Data masking

    d. Data minimization

    e. Anonymization

45. Which of the following obtains the consent of a user for the collection of only a minimal amount of personal data for an intended purpose?

    a. GDPR

    b. Terms of agreement

    c. Privacy notice

    d. Impact assessment

46. The cybersecurity team has set up a honeypot to track the attack vector of a newly released malware. As they review the virus, they notice that the hash value of the malware changes from host to host. Which of the following types of malware have been detected?

    a. Virus

    b. RAT

    c. Worm

    d. Logic bomb

    e. Polymorphic virus

47. The cybersecurity team has looked at the latest trends and identified that there has been an increase in brute-force attacks. Which of the following is a random value that can be appended to the stored password to make it more difficult for a brute-force password attack to be carried out?

    a. Obfuscation

    b. Nonce

    c. Data masking

    d. Salting

48. You are the security administrator for a software manufacturer and recently you stopped two new products from being sold as you found security flaws. Which of the following was not completed properly when the software was being developed? At what stage should more action have been taken?

    a. Software auditing

    b. Quality assurance

    c. Code signing

    d. Staging

    e. Development

    f. Testing

49. An auditor is carrying out an annual inspection of a SCADA network and finds that the programmable logic controllers (PLCs) have not been updated since last year. Upon further investigation, it is discovered that the company manufacturing these PLCs has gone into liquidation, making these controls end-of-life systems. The manufacturer is currently looking for another company to make an upgraded PLC. Which of the following recommendations should the auditor make to the management team to mitigate the risk in the short term?

    a. Remove the PLCs from the manufacturing infrastructure.

    b. Produce their own updated PLCs for the firmware.

    c. Set up a SIEM system for real-time monitoring of the SCADA system.

    d. Place the PLCs in a VLAN.

50. The auditor has carried out an inspection of the finance department and has made recommendations that the file server holding the financial data and the desktops of the financial department should use IPsec to secure the sessions between them. The network administrator is going to ensure that only the payload is encrypted. What did the security analyst recommend?

    a. IPsec in tunnel mode

    b. IPsec in split-tunnel mode

    c. IPsec in transport mode

    d. IPsec in full-tunnel mode

Mock Exam 1 Assessment

1. Answer: c

   Concept: A self-signed certificate is the cheapest certificate for internally facing servers.

2. Answer: c

   Concept: Closed/proprietary threat intelligence is funded by the company producing the report. More money would have been spent on creating the report and it will provide more accurate information as this information will be sold on to other companies.

3. Answer: c

   Concept: The logger command allows you to insert comments into a log file.

4. Answer: b

   Concept: The harvester is written in Python and allows you to search and collate the email addresses of a company on search engines such as Google.

5. Answers: a, b, c, d

   Concept: Telnet, curl, Dimitri, nmap, and nc can all be used for banner grabbing.

6. Answer: d

   Concept: When a new security update has been released, threat hunting is the process of searching current and historical logs for the symptoms of an attack.

7. Answer: b

   Concept: If it is end-of-life, the vendor will not produce any updates, but will sell the limited spare parts that they still have. With end-of-service, the vendor stops everything – no spare parts, nothing.

8. Answer: d

   Concept: Third-party authentication is federation services that use SAML.

9. Answer: c

   Concept: **Payment Card Industry Data Security Standard** (**PCI DSS**) deals with card payments.

10. Answer: c, e

    Concept: Data at rest is protected by FDE and access to the mobile telephone can be protected by screen locks and strong passwords.

11. Answer: d

    Concept: MAC is used as the access method for classified data and the security administrator is responsible for giving users access to the data once the person has been vetted and access is justified.

12. Answer: c and d

    Concept: A certificate needs to be valid and trusted by the computer.

13. Answer: c

    Concept: Only CRL and OCSP can provide certificate validation. Normally, if the CRL is going slow, you would implement an OCSP. In this case, if you remove the CRL, you need to implement an OCSP.

14. Answer: c

    Concept: Pivoting involves using a weak host to launch an attack further in the network. In virtualization, it is called VM Escape.

15. Answer: b

    Concept: This shows 45,000 bytes of data. It should have been 32 bytes. It is too much data, therefore a buffer overflow.

16. Answer: b

    Concept: Continuous monitoring detects system failure and any security breaches.

17. Answer: c

    Concept: SOC 2 reports produce a very detailed report on the internal controls of a company relating to security, data processing, and the handling of user's data to ensure it is confidential and privacy is maintained.

18. Answer: a

    Concept: Tokenization replaces data with a token that links to a payment provider who holds the data. This is better than encryption as it is stateless, whereas with encryption the keys are held locally.

19. Answer: a

    Concept: IPSec in tunnel mode is used externally on a VPN where both the header and the payload are encrypted.

20. Answer: b

    Concept: **Cloud Security Alliance Cloud Controls Matrix** (**CCM**): This is designed to provide a security principles guide for cloud vendors and potential cloud customers to assess the overall risk of a cloud provider.

21. Answer: b

    Concept: The risk register lists the risks, each risk has an owner, and the owner will decide to accept, mitigate, transfer, or avoid the risk.

22. Answer: c

    Concept: An end-of-life system is no longer supported by the vendor and no patches will be made.

23. Answer: d

    Concept: When a disaster hits, the amount of time a company can operate without access to its data is called the **Recovery Point Objective** (**RPO**).

24. Answer: b, d

    Concept: Nmap is used to create an inventory and can tell what operating system a host has and what services it is running. Netstat can tell which services are running through its port number.

25. Answer: b

    Concept: IaaS provides bare-metal hardware. Then, you need to install the software, configure it, and patch it.

26. Answer: e

    Concept: RAID 6 uses a minimum of four disks, uses double parity, and can lose two disks.

27. Answer: c

    Concept: The data controller is responsible for ensuring that all data that is collected, and its storage, is legal and follows the compliance regulations. The data controller is responsible for investigations into data breaches.

28. Answers: b and e

    Concept: Always collect the volatile evidence before stopping a cyber-attack in order to detect the source. Volatile memory evaporates if the power is switched off. RAM is volatile and the swap/page file is where applications run when RAM is full.

29. Answer: b

    Concept: End-of-life systems are no longer operational or supported by the vendor.

30. Answer: c

    Concept: Regression testing is part of program development, and in larger companies is done by code-testing specialists.

31. Answer: d

    Concept: You can shred a whole hard drive down until it looks like powder—let someone try to put that back together again.

32. Answer: d

    Concept: DDoS and DoS attack the availability of IT systems, as they both aim to take them down.

33. Answer: b

    Concept: The RTO means that the system is now back up and running. This can also be known as the return to operational state.

34. Answer: a

    Concept: Certificate pinning prevents SSL M-I-M attacks.

35. Answer: c

    Concept: Sandboxing is where we put an application in an isolated virtual machine to test patches, or maybe just because the application is too dangerous to run on our network.

36. Answer: a, b, and f

    Concept: SAML is an XML-based type of authentication used in federation services; TOTP is also XML-based.

37. Answer: b

    Concept: The intended attack was vishing, and because he left a voicemail the actual attack was vishing, as leaving a voicemail is a vishing attack.

38. Answer: c

    Concept: Separation of duties prevents one person from authorizing the whole transaction, and also prevents fraud. The CA signs the X509 certificates.

39. Answer: b

    Concept: A router gives you access to the internet; on a computer, it is known as the default gateway.

40. Answer: b, c

    Concept: A mantrap provides a safe and controlled environment in the data center as it allows you to control access.

41. Answer: d

    Concept: Cloud providers use a zero-trust model where everybody needs to prove their identity.

42. Answer: a, c

    Concept: To obtain the volatile evidence from a cloud provider, you will need a right to audit clause.

43. Answer: b

    Concept: Risk mitigation involves reducing the risk of an attack or event. These are basically technical controls.

44. Answer: d

    Concept: Data minimization is the process of collecting only the necessary data for a purpose and then retaining it only for a period required by compliance.

45. Answer: c

    Concept: A privacy notice obtains consent to collect my personal data and only use it for the purpose that it was intended.

46. Answer: e

    Concept: A polymorphic virus mutates, therefore the hash value will change.

47. Answer: d

    Concept: Salting appends a random value to a password before it is hashed

48. Answer: b, d

    Concept: Staging is where the software is tested with real data and the quality assurance of the product should have been tested and assured prior to moving the software from staging into production.

49. Answer: d

    Concept: You can place the vulnerable PLCs into a VLAN to segment them from the network.

50. Answer: c

    Concept: IPSec in transport mode is used server to server internally where only the payload is encrypted.