Mock Exam 2

1. You are a security administrator and you wish to implement an encrypted method of authentication for your wireless network. Which of the following protocols is the most secure for your wireless network?

   a. WPA2-PSK

   b. EAP-TLS

   c. PEAP

   d. PAP

2. You work on the cybersecurity team of a large multinational corporation, and you have been alerted to an attack on the web server inside your screened subnet that is used for selling your products on the internet. You can see by running netstat that you have an unknown active connection. What should be the first step you take when investigating this incident?

   a. Isolate the web server by disconnecting it from the network to prevent further damage.

   b. Disconnect all external active connections to ensure that any attack is stopped.

   c. Run a packet sniffer to capture the network traffic to identify the attacker.

   d. Take a screenshot of the damage done to the website and report the incident to the police.

3. I need to purchase a certificate that I can install on five internet-facing mail servers. Which of the following is the most cost-effective solution?

   a. PEM certificate

   b. Wildcard certificate

   c. Subject Alternative Name (SAN) certificate

   d. Root certificate

4. You are the operational manager for a financial company that has just suffered a disaster. Which of the following sites will you choose to be fully operational in the smallest amount of time?

   a. Cold site

   b. Warm site

   c. Hot site

   d. Off site

5. The serious crimes agency has just taken control of a laptop belonging to a well-known criminal that they have been trying to track down for the last 20 years. They want to ensure that everything is done by the book and that no errors are made. What is the first step in their forensic investigation, prior to starting the chain of custody?

   a. Make a system image of the laptop.

   b. Place it in a polythene bag and seal it.

   c. Hash the data so that data integrity is assured.

   d. Ask for proof of ownership of the laptop.

6. If an attacker is looking for information about the software versions that you use on your network, which of the following tools could they use? Select all that apply:

   a. Netstat

   b. Port scanning

   c. Nmap

   d. The harvester

7. Footage of people relaxing in their homes started appearing on the internet without the knowledge of the people being filmed. The people being filmed were warned by relatives and co-workers, resulting in an enquiry being launched by the police. Initial evidence reported a similarity in that they had all recently purchased IoT devices, such as health monitors, baby monitors, smart TVs, and refrigerators. Which of the following best describes why the attacks were successful?

   a. The devices' default configurations had not been changed.

   b. Their houses had been broken into and hidden cameras were installed.

   c. The victims' wireless networks were broadcasting beyond the boundaries of their homes.

   d. The manufacturers of the devices installed hidden devices, allowing them to film.

8. You are the network administrator for an IT training company that has over 20 training rooms that are all networked together in their Miami office. Last week they suffered an attack from the internet. What solution should be deployed to prevent this in the future?

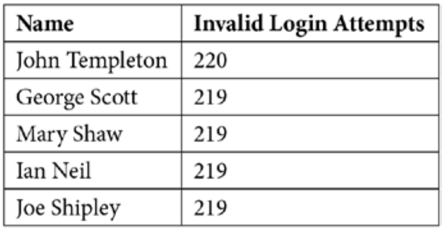
   a. Create a VLAN on the switch and put the corporate admin team in the VLAN.

   b. Install a router in the LAN and place the corporate admin team in the new subnet.

   c. Create a NAT from the firewall and put the corporate machines in that network.

   d. Install a proxy server.

9. A security administrator looked at the top five entries from a report received from a SIEM server that showed the following output:



Name	Invalid Login Attempts
John Templeton	220
George Scott	219
Mary Shaw	219
Ian Neil	219
Joe Shipley	219

   What type of attack did the SIEM system discover:

   a. Password history

   b. Password spraying

   c. RAT

   d. Dictionary attack

10. Your organization has many different ways of connecting to your network, ranging from VPN and RAS to 802.1x authentication switches. You need to implement a centrally managed authentication system that will record periods of access. Select the two most suitable methods of authentication:

    a. PAP

    b. TACACS+

    c. NTLM

    d. RADIUS

11. From a security perspective, what is the major benefit of using imaging technology, such as Microsoft WDS server or Symantec Ghost, on image desktop computers and laptops that are being rolled out?

    a. It provides a consistent baseline for all new machines.

    b. It ensures that all machines are patched.

    c. It reduces the number of vulnerabilities.

    d. It allows a non-technical person to roll out the images.

12. A company that is allowing people to access their internet application wants the people who log in to the application to use an account managed by someone else. An example of this is using their Facebook account with a technology called OpenID Connect. Which of the following protocols is this based on? Select the best choice:

    a. Kerberos

    b. SAML

    c. OAuth 2.0

    d. Federation Services

13. A security administrator has discovered that members of the sales team are connecting their own laptops to the company network without permission. What type of threat to the network have they discovered?

    a. Malicious insider

    b. BYOD

    c. Shadow IT

    d. Competitor

14. You are the security administrator for a medium-sized company that needs to enforce a much stricter password policy via group policy. The aims of this policy are to do the following:

    - Prevent using the same password within 12 password changes.

    - Ensure that users cannot change the password more than once a day.

    - Prevent weak passwords or simple passwords, such as 123456 or password, from being used.

    Select the options that you will need to fulfill all of these goals:

    a. Enforce password history

    b. Minimum password length

    c. Passwords must meet complexity requirements

    d. Minimum password age

    e. Maximum password length

15. You provide a service for people who have recently fulfilled their contract with their mobile phone provider to unlock their phone and then install third-party applications on it. They will then no longer be tied to using the mobile phone vendor's app store. Which of the following techniques will you use to achieve this? Select all that apply:

    a. Tethering

    b. Sideloading

    c. Slipstreaming

    d. Jailbreaking or rooting

    e. Degaussing

16. Which of the following is a standard for data privacy and handling?

    a. SSAE

    b. NIST

    c. PCI DSS

    d. GDPR

    e. ISO 31000

17. You are the security administrator of a multinational company that has recently prevented brute-force attacks by using account lockout settings with a low value using group policy. The CEO of the company has now dictated that the company will no longer use account lockout settings as he read an article about it and got the wrong impression. Facing this dilemma, how can you ensure that you can make it more difficult for brute force to be successful?

    a. Obfuscation

    b. Salting

    c. XOR

    d. ROT 13

18. You want to protect the admin password for a wireless router. Which of the following wireless features would be most appropriate to achieve this objective?

    a. WPA2-Enterprise

    b. TKIP

    c. WPS

    d. PSK

    e. CCMP

19. Why would a network administrator install a Network Intrusion Detection System (NIDS)? Select the two best options.

    a. It identifies vulnerabilities.

    b. It identifies new network hosts.

    c. It identifies viruses.

    d. It identifies new traffic patterns.

    e. It identifies new web servers.

20. A web server was the victim of an integer overflow attack. How could this be prevented in the future?

    a. Install a proxy server.

    b. Install a SQL injection.

    c. Input validation on forms.

    d. Install a web application firewall.

21. An attacker managed to access a guest machine and then attacked the database server and managed to exfiltrate the credit card details of 20,000 users. What type of attack did they carry out?

    a. VM escape

    b. VM sprawl

    c. System sprawl

    d. VM containerization

22. Which of the following attacks cannot be detected by any monitoring systems?

    a. Pass-the-hash

    b. Man-in-the-middle

    c. Zero-day virus

    d. Smurf attacks

23. You are the system administrator for a multinational company that wants to implement two-factor authentication. At present, you are using facial recognition as the method of access. Which of the following would allow you to obtain two-factor authentication? Select all that apply:

    a. Palm reader

    b. Signature verification

    c. Thumb scanner

    d. Gait

    e. Iris scanner

24. The security auditor has just visited your company and is recommending change management to reduce the risks from the unknown vulnerabilities of any new software introduced into the company. What will the auditor recommend for reducing the risk when you first evaluate the software? Select the best two practices to adopt from the following list:

    a. Jailbreaking

    b. Sandboxing

    c. Bluesnarfing

    d. Chroot jail

    e. Fuzzing

25. You are the owner of a small business that has just installed a terminal for allowing payment by credit/debit card. Which of the following regulations must you adhere to?

    a. SSAE

    b. NIST

    c. PCI DSS

    d. GDPR

    e. ISO 31000

26. You are the security administrator for a multinational corporation and you recently carried out a security audit. Following the audit, you told the server administrators to disable NTLM and enable Kerberos on all servers. Which of the following types of attack best describes why you took this action?

    a. It will improve the server's performance.

    b. To prevent a man-in-the-middle attack.

    c. To prevent a pass-the-hash attack.

    d. To prevent a poodle attack.

27. The political adviser to the Prime Minister of the United Kingdom has returned from the two months of summer break that all staff are entitled to. He has applied for an immediate transfer to another department, stating that his health is bad, and the job was far too intense. When his replacement arrives, he finds that, during the summer recess, the political adviser has shredded all documents relating to a political inquiry that has involved his cousin. The police are immediately called in and say that they cannot prosecute the political adviser due to a lack of evidence. What precautions could the Houses of Parliament security team take to prevent further events such as this from happening in the future?

    a. Create a change management document to ensure that the receptionists are more vigilant to people coming in out of hours.

    b. Enforce time-based access restrictions so that nobody can access the IT systems during summer breaks.

    c. Enforce separation of duties to ensure that any document that is destroyed has been witnessed by a second person.

    d. Enforce mandatory vacations to prevent him coming in during the recess.

28. You are the administrator for a large multinational organization. You wish to purchase a new biometric system. Which of the following is a critical factor when making the purchase?

    a. High FAR

    b. Low FRR

    c. Low FAR

    d. Low CER

    e. High CER

    f. High FRR

29. You work in the forensics team of a very large multinational corporation, where an attack has happened across three different sites in two different countries. You are now going to install a SIEM server to collect the following log files from all of the locations.

    - Security logs
    - DNS logs
    - Firewall logs
    - NIPS logs
    - NIDS logs

    What is the first action that you need to take before collating these logs?

    a. Apply time normalization to these logs.

    b. Copy them into a worm drive so that they cannot be tampered with.

    c. Sort out the sequence of events by site.

    d. Install a Network Time Protocol (NTP) server.

30. You are working for the serious crimes unit of the United Nations and have been given a laptop to investigate. You need to ensure that the evidence you are investigating has not been tampered with during your investigation. How are you going to prove this to the court when it is time to present your findings? Which of the following techniques will you adopt to best prove this? Select all that apply:

    a. MD5

    b. 3DES

    c. SHA1

    d. Blowfish

31. Fifteen developers are working on producing a new piece of software. After 4 weeks, they all submit the code that they have produced, and it has just been moved into the development phase of the software development. All of this code will be automated. What has just been carried out?

    a. Continuous validation

    b. Continuous monitoring

    c. Continuous integration

    d. Continuous development

    e. Automated courses of action

32. You are the security administrator for a multinational corporation that has an Active Directory domain. What type of attack uses HTML tags with JavaScript inserted between the `<script>` and `</script>` tags?

    a. Cross-site scripting

    b. Man-in-the-middle

    c. Cross-site forgery attack

    d. SQL injection

33. You are the system administrator for an Active Directory domain and deal with authentication on a daily basis. Which of the following would you use as multifactor authentication?

    a. Smart card

    b. Kerberos

    c. WPS

    d. TOTP

34. A company has just installed a new wireless network and has found that some devices are interfering with other wireless devices. Which of the following have the administrators failed to carry out? Choose the best two.

    a. Heat map

    b. Checking wireless channels

    c. Site survey

    d. Low-power directional antennas

35. You are the security administrator for a multinational company, and you know that one of your X509 certificates, used in at least 300 desktop machines, has been compromised. What action are you going to take to protect the company, using the least amount of administrative effort?

    a. Email the people involved and ask them to delete the X509 from their desktop immediately.

    b. Carry out certificate pinning to prevent the CA from being compromised.

    c. Revoke the root CA X509 so it is added to the CRL.

    d. Revoke the X509 so it is added to the CRL.

36. A biometric system has been letting in unauthorized users ever since it had a patch upgrade. Which of the following is being measured?

    a. CER

    b. FAR

    c. FRR

    d. CVE

37. Which of the following is footprinting?

    a. Creating a list of approved applications

    b. Listing network connections

    c. Creating a diagram about network connections and hosts

    d. A list of approved applications

38. You need to install a new wireless access point that should be as secure as possible, while also being backward compatible with legacy wireless systems. Which of the following do you choose to implement?

    a. WPA2 PSK

    b. WPA

    c. WPA2 CCMP

    d. WPA2 TKIP

39. You are the security administrator for a multinational corporation based in Miami, and your company has recently suffered a replay attack. Following lessons learned, you have decided to use a protocol that uses timestamps and USN to prevent replay attacks. Which of the following protocols is being implemented here? Select the best answer:

    a. Federation Services

    b. EAP-TLS

    c. Kerberos

    d. RADIUS Federation

40. A company recently suffered a break-in, where the company's research and development data was stolen, and the assembly line was damaged. Which of the following threat actors is most likely to have carried this out?

    a. A criminal syndicate

    b. A competitor

    c. A script kiddie

    d. A nation state

41. You are the new IT director of a small, family-owned business that is rapidly expanding. You have submitted your annual budget for the IT team and the owners of the company want to know why you have asked for funds for vendor diversity. They have asked you to provide two good reasons as to why they should grant you the funds. Which of the following are the most suitable reasons why you wish to implement vendor diversity?

    a. Reliability.

    b. Regulatory compliance.

    c. It is a best practice in your industry.

    d. Resilience.

42. You are the network administrator for a large multinational corporation, and you have captured packets that show that the administrators' credentials between their desktop and the network devices are in clear text. Which of the following protocols could be used to secure the authentication? Select the best choice.

    a. SNMP V 3

    b. Secure Shell

    c. SCP

    d. SFTP

43. You are the auditor of a large multinational corporation and the SIEM server has been finding vulnerabilities on a server. Manual inspection proves that it has been fully hardened and has no vulnerabilities. What are the two main reasons why the SIEM server is producing this output?

    a. There was a zero-day virus.

    b. False negatives.

    c. False positives.

    d. The wrong filter was used to audit.

44. You are the purchasing manager for a very large multinational company, and you are looking at the company's policy of dealing with the insurance of laptops. Last year, the company lost a record number of laptops. Your company is losing 10 laptops per month and the monthly insurance cost is $10,000. Which of the following laptop purchases would prevent you from purchasing insurance?

    a. A budget laptop at $1,300 each

    b. A budget laptop at $1,200 each

    c. A budget laptop at $1,000 each

    d. A budget laptop at $1,001 each

45. Which of the following is a measure of reliability?

    a. MTTR

    b. MTBF

    c. MTTF

    d. RPO

46. A research and development computer that holds trade secrets needs to be isolated from other machines on the network. Which of the following is the best solution?

    a. VLAN

    b. PVC

    c. Air gap

    d. Containment

47. Which of the following constitutes risk transference? Choose two:

    a. Outsourcing your IT support

    b. Purchasing anti-virus software

    c. Identifying and classifying the asset

    d. Purchasing cybersecurity insurance

48. Which of the following are the characteristics of a third-party to third-party authentication protocol that uses XML-based authentication?

    a. Single sign-on (SSO)

    b. Kerberos

    c. SAML

    d. Secure Shell

49. A cybersecurity administrator is looking at a customer database and has noticed the following against the credit card of a customer:

```
**** **** **** 3456
```

    What has the administrator come across?

    a. Tokenization

    b. Obfuscation

    c. Data masking

    d. XOR

50. A security administrator found that a domain controller was infected by a virus. They isolated it from the network and then removed the virus and turned off the telnet service? Which of the following has the administrator just carried out?

    a. Containment

    b. Eradication

    c. Recovery

    d. Lessons learned

Mock Exam 2 Assessment

1. Answer: b

   Concept: EAP-TLS is a secure wireless authentication protocol, as it uses certificates. An X509 certificate is installed on the endpoint. This is the most secure EAP standard.

2. Answer: c

   Concept: The first stage in any attack is to capture the volatile evidence. In this incident, you would capture the network traffic to identify the source of the attack.

3. Answer: b

   Concept: A wildcard certificate can be used on multiple servers, normally those that are internet facing.

4. Answer: c

   Concept: The hot site should be up and running with data that has been replicated.

5. Answer: a

   Concept: The first step is to create a system image or, if it is a hard drive, create a forensic copy.

6. Answer: c

   Concept: A **Network mapper** (**Nmap**) can identify new hosts on the network, identify what services are running, and identify what operating systems are installed. It can also be used for banner grabbing.

7. Answer: a

   Concept: IoT home-based automated devices should have the default configurations of the username and password changed. Most users do not realize that these passwords exist.

8. Answer: c

   Concept: A NAT hides the internal network from external users.

9. Answer: b

   Concept: Password spraying is where an attacker obtains a list of employees and then tries common passwords against each account.

10. Answer: b and d

    Concept: AAA servers are used for centralized authentication as they provide authentication, authorization, and accounting. They can record all log-ins and log-outs in a database.

11. Answer: a

    Concept: When you build an image, all of the applications will have the same settings and updates and therefore will be consistent. A baseline consists of the applications that are installed at the current time.

12. Answer: c

    Concept: OAuth 2.0 is the industry-standard protocol for authorization. It is used by OpenID Connect, where people can be authenticated using their Facebook or Google account.

13. Answer: c

    Concept: A shadow IT threat is where someone connects their device to a private network without permission.

14. Answers: a, c, d

    Concept: The password history is the number of passwords that you need to remember before you can reuse them. Password complexity requires users to use three of the four following characters in the password: lowercase, uppercase, numbers, and special characters not used in programming. A minimum password age set to 1 means that you can change the password only once a day, preventing password rotation until you get back to the original password.

15. Answers: b and d

    Concept: Sideloading involves loading third-party applications onto an unlocked mobile Phone. Jailbreaking (iOS), or rooting (Android), is where the phone has been unlocked, removing the vendor's restrictions on the mobile phone.

16. Answer: d

    Concept: GDPR is a framework for data protection law ensuring the privacy rights of individuals. It deals with data privacy and data sharing.

17. Answer: b

    Concept: Salting appends random characters to a password before it is hashed. As the passwords are then longer, brute-force attacks need more processing and computation resources to crack them.

18. Answer: e

    Concept: CCMP uses AES for encryption and is the strongest wireless security.

19. Answer: b, d

    Concept: A NIDS uses sensors and collectors to identify changes to the network.

20. Answer: c

    Concept: Input validation prevents buffer-overflow attacks, integer-overflow attacks, and SQL injection by restricting the input to a certain format.

21. Answer: a

    Concept: VM escape can be used for a lateral attack on the virtual host or the other virtual machines.

22. Answer: c

    Concept: A zero-day virus is a newly released virus, and no monitoring system can detect it until it receives an update in about 7 days' time. There are no patches for it either.

23. Answer: b and d

    Concept: Facial recognition is something you use for authentication. b and d are both something you do – you have a unique signature, and your gait is how you walk.

24. Answer: b and d

    Concept: Sandboxing and chroot jail (Linux version) allow you to isolate an application inside a virtual guest machine.

25. Answer: c

    Concept: **Payment Card Industry Data Security Standard** (**PCI DSS**) lays out the regulations for the handling and storage of financial information.

26. Answer: c

    Concept: Disabling NTLM or enabling Kerberos will prevent pass-the-hash attacks. Kerberos is the best of the two as passwords are held in an encrypted database.

27. Answer: b

    Concept: Time-based access restrictions would have prevented someone from accessing the system during the holidays.

28. Answer: d

    Concept: When the FAR and FRR are equal, this is known as the CER. A system with a low CER is the best choice as it has very few errors.

29. Answer: d

    Concept: We need to install an NTP server to synchronize the time of all of the servers so that the events can be put into a sequence of events.

30. Answer: a and c

    Concept: Hashing proves data integrity. SHA1 and MD5 are both hashing algorithms.

31. Answer: c

    Concept: Continuous Integration is where code from multiple sources is integrated together.

32. Answer: a

    Concept: **Cross-Site Scripting** (**XSS**) uses HTML tags or JavaScript.

33. Answer: a

    Concept: A smart card is "something you have," inserting the card into the reader is "something you do," and then when you insert the PIN, it is "something that you know."

34. Answers: a, c

    Concept: A site survey should be carried out prior to installing a wireless network as it maps out all of the items that would interfere with a wireless connection. A heat map shows the coverage with blue/green areas showing poor connectivity and red showing great connectivity.

35. Answer: d

    Concept: Once a certificate has been compromised, it should immediately be revoked so it is added to the CRL.

36. Answer: b

    Concept: Unauthorized users are allowed. Look at the middle initial in FAR – it is A for allow.

37. Answer: c

    Concept: Footprinting maps out network topology including active hosts.

38. Answer: d

    Concept: WPA2 is the most secure and TKIP is backward compatible. WPA also works with legacy but is not the best choice.

39. Answer: c

    Concept: Kerberos issues tickets for authentication, and each change has a different **Updated Sequence Number** (**USN**) and timestamps. It prevents both replay and pass-the-hash attacks.

40. Answer: b

    Concept: The R&D department creates a lot of the company's trade secrets; therefore, a competitor would steal them to beat you to the marketplace. If they damaged your production line, it would prevent you from getting a product to market.

41. Answer: a and d

    Concept: Vendor diversity involves getting a service from two different providers at the same time. Vendor diversity provides reliability and resilience. For example, if broadband from one provider fails, then the second provider's broadband should still be up and running.

42. Answer: b

    Concept: **Secure Shell** (**SSH**) is used for secure remote access and credentials are protected.

43. Answer: c and d

    Concept: If we are using the wrong configuration for the SIEM server, we will get poor monitoring, resulting in false positives. This would also happen if you scanned the wrong type of host.

44. Answer: c

    Concept:

```
SLE = ALE/ARO
ALE = 12 x 10,000 = $120,000
ARO = 12 X 10 = 120 laptops a year
Single loss expectancy = $120,000/120 = $1000
```

    Explanation: The cost of losing the laptops is $120,000, the same as purchasing the insurance. You should not take out the insurance in the hope that next year you may lose fewer laptops, as a record number of laptops has already been lost.

45. Answer: b

    Concept: **Mean Time Between Failures** (**MTBF**) is the measure of the number of failures. If I purchased a car and it broke down every day for the next week, I would take it back, as it would be unreliable.

46. Answer: c

    Concept: An airgap isolates a computer from the network as it has no physical or wireless connections. The only way to extract data is by removable media.

47. Answers: a, d

    Concept: Risk transference is where you transfer the responsibility of the risk to a third party, purchasing insurance of any kind and outsourcing your IT are examples.

48. Answer: c

    Concept: Federation services is a third-party-to-third-party authentication method that uses SAML, an XML-based method for authentication. SAML passes credentials to the **Identity Provider** (**IdP**).

49. Answer: c

    Concept: Data masking masks all or some of the data held in a field.

50. Answer: b

    Concept: Removing viruses and turning off services are carried out at the eradication phase.

Assessment

Chapter 1 – Understanding Security Fundamentals

1. The three components of the CIA triad are confidentiality, where the data is encrypted, integrity, where the data uses hashing, and availability, where the data is available, for example, by restoring data from a backup.
2. A CCTV camera without any film inside is used as a deterrent, as criminals would not know that there is no film inside.
3. Confidentiality means preventing other people from viewing the data; the best way to keep data confidential is to encrypt it.
4. The best way to control entry into a data center is to install a mantrap.
5. An air gap is where a computer or device has no physical connections, such as Wi-Fi, or an Ethernet cable isolating it from your network.
6. The three control categories are managerial, operational, and physical.
7. Choose three of the following physical controls: Lighting, cameras, robot sentries, fences, gate signage, industrial camouflage, security guards, badges, key management, proximity card, tokens, biometric locks, electronic locks, burglar alarms, smoke detectors, internal protection, conduits, HVAC, cable locks, airgap, laptop safe, USB data blocker, vault, and Faraday cage.
8. Researching an incident requires detective controls where all of the evidence is gathered.
9. Hashing provides data integrity where the hash value is measured before and after accessing data. If the values match, it has integrity.
10. Corrective controls are the actions you take to recover from an incident. You may have to restore data from a backup.

11. Firewall rules are designed to mitigate risk and they are technical controls.
12. A smart card, a CAC card, or a PIV card are all used in conjunction with a PIN.
13. In a MAC model, the custodian stores and manages the data. The administrator grants access to the data.
14. In a DAC environment, the data owner decides who has access to the data.
15. Least privilege is the process of giving an employee the minimal permissions to perform their job.
16. The Linux permission of `764` gives the owner read, write, and execute access, the group read and write access, and other (users) read access.
17. This is called rule-based access control where the access is applied to the whole department.
18. The two people from finance are using role-based access control where a subset of a department is carrying out a subset of duties.
19. The defense in depth model has multiple layers to protect data and resources. If the outer layer fails, then the next layer should perform the protection. Many layers need to be broken through before gaining access to the data or resource.
20. When someone leaves the company, we should disable the account and reset the password so that it cannot be used.
21. The EU GDPR regulations state that if a website that is hosted by someone in the US is accessed by someone from within the EU, that website needs to be GDPR-compliant.
22. If a company puts a right to audit clause into a contract, it gives them the right to audit the supplier at any time. This way, the company can look at the company records and check the quality of the products and materials being used.
23. Chain of custody is a record of who has collected the evidence and provides a log of who has handled the data. The original data must be intact and there must not be any break in the chain.
24. The US released The CLOUD Act so that they could obtain evidence from other countries for the purposes of an FBI investigation. The UK government released the COPOA act to seek data stored overseas and give their law enforcement faster access to evidence held by providers.
25. Stage C of Cloud Forensic Process 26 is to ascertain the type of technology behind the cloud.

Chapter 2 – Implementing Public Key Infrastructure

1. A CA has a root certificate, which it uses to sign keys.
2. You would use a private CA for internal use only; these certificates will not be accepted outside of your organization.
3. You would use a public CA for B2B activities.
4. If you were a military, security, or banking organization, you would keep the CA offline when it is not being used to prevent it from being compromised.
5. An architect would build the CA or intermediary authorities.
6. The CA would sign the X509 certificates.
7. Certificate pinning can be used to prevent a CA from being compromised and fraudulent certificates being issued.
8. If two separate PKI entities want to set up cross-certification, the root CAs would set up a trust model between themselves, known as a bridge trust model.
9. PGP uses a trust model known as a web of trust.
10. A **Certificate Revocation List** (**CRL**) is used to determine whether a certificate is valid.
11. If the CRL is going slow, an OCSP is used as it provides faster validation.
12. Certificate stapling/OCSP stapling is where a web server uses an OCSP for faster certificate authentication, bypassing the CRL.
13. A **Certificate Signing Request** (**CSR**) is a new certificate request.
14. The key escrow stores and manages private keys for third parties.
15. A hardware security module is used by the key escrow as it securely stores and manages certificates.
16. When a user's private key becomes corrupt, the DRA recovers the data by obtaining a copy of the private key from the key escrow.
17. Each certificate can be identified by its OID, which is similar to a serial number.
18. A private certificate is in P12 format with a `.pfx` extension.
19. A public certificate is in P7B format with a `.cer` extension.
20. A PEM certificate is in Base64 format.

21. A wildcard certificate can be used on multiple servers in the same domain.
22. A **Subject Alternative Name** (**SAN**) certificate can be used on multiple domains.
23. Code-signing software is similar to hashing the software and ensuring the integrity of the software.
24. Extended validation is normally used by financial institutions as it provides a higher level of trust for the X509; when it is used, the URL background turns green.
25. The Caesar cipher is a substitution cipher; an example would be ROT 4, where each letter would be substituted by a letter four characters along in the alphabet.
26. Encryption is when plain text is taken and turned into ciphertext.
27. Symmetric encryption is used to encrypt large amounts of data as it uses one key.
28. DH is an asymmetric technique that creates a secure tunnel; during a VPN connection, it is used during the IKE phase and uses UDP port `500` to create the VPN tunnel.
29. The first stage in encryption is key exchange. During asymmetric encryption, each entity will give the other entity its public key. The private key is secure and never given away.
30. Carol uses Bob's public key to encrypt the data, and then Bob will use his private key to decrypt the data. Encryption and decryption are always done by the same key pair.
31. George must obtain the old private key to decrypt the data as the encryption was done with a different key pair.
32. Janet will digitally sign the email with her private key and John will check its validity with Janet's public key, which he would have received in advance.
33. A digital signature provides both integrity and non-repudiation.
34. ECC will be used to encrypt data on a smartphone as it is small and fast and uses the DH handshake.
35. AES-256 will be used to encrypt a military mobile telephone.
36. Two key-stretching algorithms are bcrypt and PBKDF2.
37. Key stretching salts the password being stored so that duplicate passwords are never stored, and it also increases the length of the keys to make things harder for a brute-force attack.

38. Streams encrypt one bit at a time and block ciphers take blocks of data, such as 128-bit modes. A block cipher will be used for large amounts of data.
39. CBC needs all of the blocks of data to decrypt the data; otherwise, it will not work.
40. Hashing ensures the integrity of data; two examples include SHA-1 (160 bit) and MD5 (128 bit).
41. Encryption is used to protect data so that it cannot be reviewed or accessed.
42. A hash is one-way and cannot be reversed.
43. POODLE is a man-in-the-middle attack on a downgraded SSL 3.0 (CBC).
44. DHE and ECDHE are both ephemeral keys that are short-lived, one-time keys.
45. The strongest encryption for an L2TP/IPSec VPN tunnel is AES and the weakest is DES.
46. A session key ensures the security of communications between a computer and a server or a computer and another computer.
47. Data-at-rest on a laptop is protected by FDE.
48. Data-at-rest on a tablet or smartphone is protected by FDE.
49. Data-at-rest on a backend server is stored on a database, so it needs database encryption.
50. Data-at-rest on a USB flash drive or external hard drive is done via full disk encryption.
51. Data-in-transit could be secured by using TLS, HTTPS, or an L2TP/IPsec tunnel.
52. Data-in-use could be protected by full memory encryption.
53. Obfuscation is used to make the source code look obscure so that if it is stolen, it cannot be understood. It masks the data and could use either XOR or ROT13 to obscure the data.
54. Perfect forward secrecy ensures that there is no link between the server's private key and the session key. If the VPN server's key was compromised, it could not decrypt the session.
55. A collision attack tries to match two hash values to obtain a password.
56. Rainbow tables are a list of precomputed words showing their hash value. You will get rainbow tables for MD5 and different rainbow tables for SHA-1.
57. Steganography is used to conceal data; you can hide a file, image, video, or audio inside another image, video, or audio file.

58. DLP prevents sensitive or PII information from being emailed out of a company or being stolen from a file server using a USB device.
59. Salting a password ensures that duplicate passwords are never stored and makes things more difficult for brute-force attacks by increasing the key size (key stretching).It appends the salt to the password making it longer than before hashing.

Chapter 3 – Investigating Identity and Access Management

1. A password is most likely to be entered incorrectly; the user may forget the password or may have the Caps Lock key set up incorrectly.
2. When purchasing any device, you should change the default username and password as many of these are available on the internet and could be used to access your device.
3. Password history is the number of passwords you can use before you can reuse your current password. Some third-party applications or systems may call this a password reuse list.
4. Password history could be set up and combined with a minimum password age. If you set the minimum password age to 1 day, a user could only change their password a maximum of once per day. This would prevent them from rotating their passwords to come back to the old password.
5. A complex password uses three of the following: uppercase and lowercase letters, numbers, and special characters not used in programming.
6. If you set up an account lockout with a low value, such as 3, the hacker needs to guess your password within three attempts or the password is locked out, and this disables the user account.
7. A smart card is multi-factor or dual-factor as the card is something you have, and inserting it into a card reader is something you do, and the PIN is something you know.
8. A password, PIN, and date of birth are all factors that you know; therefore, it is single-factor.
9. Biometric authentication is where you use a part of your body or voice for authentication, for example, your iris, retina, palm, or fingerprint.

10. Federated services are an authentication method that can be used by two third parties; this uses SAML and extended attributes, such as an employee's ID or email address.
11. **Security Assertion Mark-up Language** (**SAML**) is an XML-based authentication protocol used with federated services.
12. Shibboleth is a small, open source Federation Services protocol.
13. **Lightweight Directory Authentication Protocol** (**LDAP**) is used to store objects in X500 format and search Active Directory objects such as users, printers, groups, or computers.
14. A distinguisher name in the ITU X500 object format is `cn=Fred`, `ou=IT`, `dc=Company`, `dc=Com`.
15. Microsoft's Kerberos authentication protocol is the only one that uses tickets. It also uses timestamps and updated sequence numbers to prevent replay attacks. It also prevents pass-the-hash attacks as it does not use NTLM.
16. A **Ticket-Granting Ticket** (**TGT**) process is where a user logs in to an Active Directory domain using Kerberos authentication and receives a service ticket.
17. Single sign-on is where a user inserts their credentials only once and accesses different resources, such as email and files, without needing to re-enter the credentials. Examples of this are Kerberos, Federation Services, or a smart card.
18. Pass-the-hash attacks exploit older systems such as Microsoft NT4.0, which uses NT LAN Manager. You can prevent this by enabling Kerberos or disabling NTLM.
19. OpenID Connect is where you access a device or portal using your Facebook, Twitter, Google, or Hotmail credentials. The portal itself does not manage the account.
20. The first AAA server is Microsoft RADIUS, using UDP port `1812` – it is seen as non-proprietary. The second is Cisco TACACS+ and uses TCP port `49`. Diameter is a more modern secure form of RADIUS that is TCP-based and uses EAP.
21. Accounting is an AAA server where they log the details of when someone logs in and logs out; this can be used for billing purposes. Accounting is normally logged into a database such as SQL. RADIUS Accounting uses UDP port `1813`.
22. A VPN solution creates a secure connection from a remote location to your corporate network or vice versa. The most secure tunneling protocol is L2TP/IPSec.
23. PAP authentication uses a password in clear text; this could be captured easily by a packet sniffer.

24. An iris scanner is a physical device used for biometric authentication.
25. Facial recognition could be affected by light or turning your head slightly to one side; some older facial recognition systems accept photographs. Microsoft Windows Hello is much better as it uses infrared and is not fooled by a photograph or affected by light.
26. Type II in biometric authentication is Failure Acceptance Rate, where people that are not permitted to access your network are given access.
27. **Time-Based One-Time Password** (**TOTP**) has a short time limit of 30–60 seconds.
28. HOTP is a one-time password that does not expire until it is used.
29. A CAC is similar to a smart card as it uses certificates, but the CAC is used by the military and has a picture and the details of the user on the front, as well as their blood group and Geneva convention category on the reverse side.
30. IEE802.1x is port-based authentication that authenticates both users and devices.
31. A service account is a type of administrative account that allows an application to have a higher level of privileges to run on a desktop or server. An example of this is using a service account to run an anti-virus application.
32. A system administrator should have two accounts: a user account for day-to-day tasks, and an administrative account for administrative tasks.
33. When you purchase a baby monitor, you should rename the default administrative account and change the default password to prevent someone from using it to hack into your home. This is known as an **Internet of Things** (**IoT**) item.
34. A privileged account is an account with administrative rights.
35. When monitoring and auditing are carried out, the employees responsible cannot be traced from more-than-one-person shared accounts. Shared accounts should be eliminated for monitoring and auditing purposes
36. Default accounts and passwords for devices and software can be found on the internet and used to hack your network or home devices. Ovens, TVs, baby monitors, and refrigerators are examples, and therefore pose a security risk.
37. The system administrator is using a standard naming convention.
38. When John Smith leaves the company, you need to disable his account and reset the password. Deleting the account will prevent access to the data he used.
39. Account recertification is an audit of user accounts and permissions that is usually carried out by an auditor. This is also referred to as a user account review.

40. A user account review ensures that old accounts have been deleted and that all current users have the appropriate access to resources and not a higher level of privilege.
41. A SIEM system can carry out active monitoring and notify the administrators of any changes to user accounts or logs.
42. Following an audit, either change management or a new policy will be put in place to rectify any area not conforming to company policy.
43. The contractor's account should have an expiry date equal to the last day of the contract.
44. Rule-based access should be adopted so that the contractors can access the company network between 9 a.m. and 5 p.m. daily.
45. Time and day restrictions should be set up against each individual's user account matching their shift pattern.
46. Account Lockout with a low value will prevent brute-force attacks.
47. Create a group called IT apprentices, and then add the apprentices, accounts to the group. Give the group read access to the IT data.
48. The credential manager can be used to store generic and Windows 10 accounts. The user therefore does not have to remember the account details.
49. The company should have disabled the account and reset the password. A user account review needs to be carried out to find accounts in a similar situation.
50. To copy and install the public key on the SSH server and add to the list of authorized keys.
51. This is where a user logs in to a device from one location, and then they log in from another location shortly afterward, where it would be impossible to travel that distance in the time between logins.
52. This is known as a risky login as I have used a secondary device to log in to Dropbox.
53. A password vault is an application that stores passwords using AES-256 encryption and it is only as secure as the master key.
54. They would use a dynamic KBA that would ask you details about your account that are not previously stored questions.
55. FAR allows unauthorized user access, and FRR rejects authorized user access.

56. Privileged Access Management is a solution the stores the privileged account in a bastion domain to help protect them from attack.
57. Some people don't realize that there are generic accounts controlling the devices that make them vulnerable to attack.
58. Some devices being used do not belong to a domain, for example, an iPad, so every connection should be considered unsafe.
59. Biometric authentication allows unauthorized users access to the system.

Chapter 4 – Exploring Virtualization and Cloud Concepts

1. Elasticity allows you to increase and decrease cloud resources as you need them.
2. **Infrastructure as a Service** (**IaaS**) requires you to install the operating systems and patch the machines. The CSP provides bare-metal computers.
3. SaaS is a custom application written by a vendor and you cannot migrate to it.
4. The major benefit of a public cloud is that there is no capital expenditure.
5. A private cloud is a single-tenant setup where you own the hardware.
6. A public cloud is multi-tenant.
7. A community cloud is where people from the same industry, such as a group of lawyers, design and share the cost of a bespoke application and its hosting, making it cost-effective.
8. The CSP is responsible for the hardware fails.
9. The CASB ensures that the policies between on-premises and the cloud are enforced.
10. On-premises is where you own the building and work solely from there.
11. A hybrid cloud is where a company is using a mixture of on-premises and the cloud.
12. Distributive allocation is where the load is spread evenly across a number of resources, ensuring no one resource is over-utilized. An example of this is using a load balancer.
13. **Security as a Service** (**SECaaS**) provides secure identity management.
14. A diskless virtual host will get its disk space from an SAN.

15. A VLAN on an SAN will use an iSCSI connector.
16. An SAN will use fast disks, such as SSDs.
17. A host holds a number of virtual machines – it needs fast disks, memory, and CPU cores.
18. A guest is a virtual machine, for example, a Windows 10 virtual machine. A snapshot can be used to roll back to a previous configuration.
19. Sandboxing is where you isolate an application for patching or testing or because it is dangerous. A chroot jail is for sandboxing in a Linux environment.
20. A snapshot is faster at recovering than any other backup solution.
21. A Type 1 hypervisor is a bare-metal hypervisor. Some examples are Hyper-V, ESX, and Xen.
22. A Type 2 hypervisor is a hypervisor that sits on top of an operating system, for example, VirtualBox, which could be installed on a Windows 10 desktop.
23. HVAC keeps the servers cool by importing cold air and exporting hot air. If a server's CPU overheats, it will cause the server to crash.
24. A community cloud is where people from the same industry share resources.
25. Cloud storage for personal users could be iCloud, Google Drive, Microsoft OneDrive, or Dropbox.
26. Fog computing is an intermediary between the device and the cloud. It allows the data to be processed closer to the device. It reduces latency and cost.
27. It allows data storage to be closer to the sensors rather than miles away in a data center.
28. A container allows the isolation of the applications and its files and libraries so that the application is independent.
29. Infrastructure as code allows you to automate your infrastructure, for example, using PowerShell DSC.
30. This is the combination of business and IT functions into a single business solution.
31. These are policies that state the actions and access levels someone has in relation to a particular resource.
32. This is where a virtual machine or host has run out of resources. The best way to avoid this is to use thin provisioning.

33. VM escape is where an attacker will use a vulnerable virtual machine to attack the host of another virtual machine. The best protection against this attack is to ensure that the hypervisor and all virtual machines are fully patched.
34. A cloud region consists of multiple physical locations called zones; data can be spread across multiple zones for redundancy.
35. Secrets management uses a vault to store keys, passwords, tokens, and SSH keys used for privilege accounts. It uses RSA 2048-bit keys to protect the secret management access key.
36. LRS replicates three copies of your data to a single physical location. This is the cheapest option. ZRS is where three copies of the data are replicated to three separate zones within your region.
37. They would be used as a form of network segmentation.
38. Resources that need access to the internet, for example, company web servers. A NAT gateway and an internet gateway would also be on these subnets.
39. Resources that should not have direct internet access, such as database servers, domain controllers, and email servers.
40. A VPN connection using L2TP/IPSec should be used to connect to a VPC.
41. The default route of `0.0.0.0` should be pointing to either the NAT gateway or the internet gateway. When network traffic does not know where to go, it will be sent to the default route as a last resort.
42. The third-party tools will offer more flexibility.

Chapter 5 – Monitoring, Scanning, and Penetration Testing

1. The white box tester can access the source code.
2. It would prevent you from monitoring or auditing an individual.
3. The gray box pen tester would be given at least one piece of information; normally they get limited data.
4. Rules of engagement must be established.
5. He would have regular meetings with the client, who would tell him if he has been discovered.

6. The scope determines whether the pen test is black, gray, or white.
7. The pen tester would give the internal IT team their IP address so that they can establish whether or not it is the pen tester or an attacker.
8. The credentialed vulnerability scan has more permissions than a non-credentialed one and has the ability to audit, scan documents, check account information, check certificates, and provide more accurate information
9. The cleanup phase is where the systems are returned back to the original state.
10. Open source intelligence; this is legal intelligence that is obtained from the public domain.
11. They fulfill the role of the attacker.
12. They fulfill the role of the defender.
13. They organize and judge the cybersecurity events, ensuring reports are accurate and the correct countermeasures are recommended.
14. They carry out the rules of both the red and blue teams; these are external consultants or auditors.
15. You must deal with the most critical vulnerabilities first.
16. When a monitoring system and manual inspection differ. For example, a SIEM system says there is an attack, and a manual inspection confirms that there is no attack.
17. When a monitoring system and manual inspection agree on events.
18. An intrusive scan will cause damage whereas a non-intrusive scan is passive and won't cause damage.
19. Regression testing is where a coding expert checks the code written for an application to ensure that there are no flaws.
20. Dynamic analysis is evaluating a program where it is running in real time.
21. The syslog server collects data from various sources in an event logging database. It filters out legitimate events and forwards the rest of the data to the SIEM server for further analysis.
22. A SIEM server puts events into chronological order. If the clocks are not synchronized, then events cannot be put into sequential order.
23. The IT team carry out threat hunting in their own systems to try and discover whether they have been subjected to a cyber attack.

Chapter 6 – Understanding Secure and Insecure Protocols

1. When using Kerberos authentication, a TGT session is established, where the user obtains an encrypted service ticket. Kerberos uses USN and timestamps to prevent replay attacks.
2. IPSec in tunnel mode is used with an L2TP/IPSec VPN session where both the AH and ESP are encrypted.
3. IPSec in transport mode is server to server on a LAN where only the ESP is encrypted.
4. SSH is a secure protocol that replaces Telnet.
5. A router connects external networks and routes IP packets.
6. A switch is an internal device connecting computers being used in the same location.
7. Spotify is a subscription service where the user pays a monthly fee. It is a pay-per-use model.
8. Port security is where a port on a switch is disabled to prevent someone from using a particular wall jack.
9. 802.1x authenticates users and devices connecting to a switch. Normally, the user or device has a certificate to authenticate them without the need to disable ports on the switch. An unauthorized user is prevented from using the port as they have no certificate.
10. The three portions of a distinguished name from left to right are CN, OU, and then DC.
11. DNSSEC, which produces RRSIG records that prevent DNS poisoning.
12. A computer might not receive an IP address from a DHCP server due to resource exhaustion or network connectivity.
13. Both a SIEM server and a Microsoft domain controller using Kerberos authentication are dependent on an NTP server to keep the clock times on the hosts up to date. Otherwise, the SIEM server cannot put events into chronological order and Kerberos clients cannot log in.
14. The building administrator would normally have companies located in the same physical location connected to the same switches. They could provide departmental isolation by using VLANs.

15. The spanning tree protocol prevents switches from looping, which slows the switch down.
16. A network administrator could use SMTP v3 to securely collect the status and reports from network devices.
17. A network administrator could use AES as the strongest protocol for an L2TP/IPSec VPN as it can use 256 bit.
18. A pass-the-hash attack is a hash collision attack against NTLM authentication. Kerberos prevents this attack and Kerberos uses Active Directory, which stores the passwords in an encrypted database.
19. **Transport Layer Security** (**TLS**) protects data in transit.
20. S/MIME can be used to digitally sign emails between two people.
21. SRTP is used to secure videoconferencing traffic.
22. SIP is used to manage internet-based calls and can be used with Skype to put calls on hold and transfer them.
23. LDAP uses TCP port `389` and is used to manage directory services. It can be replaced by LDAPS TCP port `636`, which is more secure.
24. The format is NETBIOS, where the name is up to 15-characters long with a service identifier. In this example, the host is called Ian; `<00>` indicates the workstation service and `<20>` indicates the server service.
25. FTPS is used to transfer large files as it uses two ports: `989/990`.

Chapter 7 – Delving into Network and Security Concepts

1. The web application firewall is normally installed on a web server as its job is to protect web applications from attack.
2. Implicit Deny is used by both the firewall and the router. If there is no allow rule they get the last rule which is deny all. This is known as Implicit Deny.
3. **Unified Threat Management** (**UTM**) is a firewall that provides value for money as it can provide URL filtering, content filtering, and malware inspection, as well as firewall functionality.
4. A router connects different networks together and works at Layer 3 of the OSI reference model.

5. A switch connects users on an internal network, normally in a star topology.
6. A **Network Address Translator** (**NAT**) hides the internal network from those on the external network.
7. An inline NIPS is where the incoming traffic passes through and is screened by the NIPS.
8. A **Host-Based IPS** (**HIPS**) is installed inside the guest virtual machine to protect it from attacks.
9. A **Network-Based IPS** (**NIPS**) is placed behind the firewall as an additional layer of security. The firewall prevents unauthorized access to the network.
10. A NIPS can passively monitor the network as it can fulfill the functionality of a NIDS if there is no NIDS on your network.
11. A signature-based NIDS works off a known database of variants, whereas an anomaly-based one starts with the database and can learn about new patterns or threats.
12. A passive device that sits inside your network is a NIDS.
13. If one of the monitoring systems reports a virus and you manually check and find no virus, this is known as a false positive.
14. You should enable port security, where you turn the port off on the switch. This will prevent further use of the wall jack.
15. To prevent a rogue access point from attaching to your network, you would enable 802.1x on the switch itself. 802.1x ensures that the device is authenticated before being able to use the post.
16. A managed switch uses 802.1x, which authenticates the device but does not disable the port when port security merely disables the port. 802.1x, therefore, provides more functionality.
17. Web caching on a web server keeps copies of the web pages locally, ensuring faster access to the web pages and preventing the need to open a session to the internet.
18. The purpose of a VPN is to create a tunnel across unsafe networks from home or a hotel to the workplace.
19. In the IKE phase of an IPSec session, Diffie Hellman using UDP port `500` sets up a secure session before the data is transferred.
20. The purpose of a VPN concentrator is to set up a secure session for a VPN.

21. The most secure VPN tunnel is L2TP/IPSec, which uses AES encryption for the ESP.
22. IPSec in tunnel mode is used across the internet or external networks, and IPSec in transport mode is used between hosts internally.
23. When setting the site-to-site VPN, it should be used in always-on mode as opposed to dial-on-demand.
24. A load balancer should be used to manage a high volume of web traffic as it sends the requests to the least-utilized node that is healthy.
25. SDN is used in a virtual environment when the routing requests are forwarded to a controller.
26. The screened subnet is a boundary layer that hosts an extranet server; it is sometimes known as the extranet zone. It used to be called the DMZ.
27. If you set up a honeypot, which is a website with lower security, you will be able to monitor the attack methods being used and then be able to harden your actual web server against potential attacks.
28. Network access control ensures that devices connecting to your network are fully patched. There are two agents: one that is permanent and another that is dissolvable that is for single use.
29. A SIEM server can correlate log files from many devices and notify you of potential attacks.
30. If data is backed up to a **Write-Once Read-Many** (**WORM**) drive, the data cannot be deleted or altered.
31. A port mirror can make a copy of the data going to a port and divert it to another device for analysis. A tap is another device that can be used for the same purpose. However, a tap is more expensive.
32. DNSSEC creates RRSIG records for each DNS host and a DNSKEY record used to sign the KSK or ZSK.
33. An IPSec packet has the authenticated header that uses either SHA-1 or MD5 and an **Encapsulated Payload** (**ESP**) that uses DES, 3DES, or AES.
34. If you cannot get an IP address from a DHCP server, you would receive a `169.254.x.x` IP address. This is known as APIPA. This could be caused by network connectivity or resource exhaustion.
35. It is an IP version 6 address and you can simplify it by changing the leading zeros to `2001:123A::ABC0:AB:DCS:23`.

36. An HTML5 VPN has no infrastructure to be set up as it uses certificates for encryption.
37. This would be IPSec in tunnel mode and would be used externally.
38. The purpose of a jump server is to allow a remote SSH session to a device or a virtual machine in a screened subnet or the cloud.
39. This is where the host is sent to the same server for the session.
40. Both of the load balancers are working close to capacity and if one of these load balancers fails, then the users would find that the traffic is slower.
41. A VLAN can be used for departmental isolation on the same switch.
42. East-West traffic moves laterally between servers within a data center.
43. A zero-trust network is where nothing is trusted, and every user or device must prove their identity before accessing the network. This would be used in the cloud.
44. Angry IP is an IP scanner that would scan an IP range to determine hosts that are active or inactive.
45. `curl` and `nmap` could be used for banner grabbing.
46. The harvester tool is used to collect the email addresses of a particular domain from search engines such as Google.
47. They can use the `dnsenum` tool.
48. It allows anonymous port scanning so that it cannot be traced back to you
49. You could use the tool called `cuckoo` to carry out this activity.
50. This is to prevent rogue DHCP servers from operating openly on your network.
51. It could be resource exhaustion, where the DHCP server has run out of IP addresses or it could be network connectivity between the client and the DHCP server.

Chapter 8 – Securing Wireless and Mobile Solutions

1. Visitors and employees on their lunchtime break might access a guest wireless network.
2. The FAT wireless controller is standalone; it has its own setting and DHCP addresses configured locally. A thin wireless controller pushes out the setting to multiple WAPs.

3. The WAP master password is the admin password, and it should be encrypted to protect it.
4. Wi-Fi Analyzer can troubleshoot wireless connectivity and discover the SSID inside a packet going to the WAP.
5. MAC filtering controls who can access a WAP. If your MAC address is not added to the WAP, then you are denied access.
6. To prevent interference by overlapping the wireless channels.
7. He would ensure that the WAPs are placed where there is no interference.
8. No, because it is not secure.
9. WEP is the weakest as it only has 40-bit encryption.
10. You are giving them the **Pre-Shared Key** (**PSK**).
11. It is WPA2-CCMP as it uses AES encryption that is 128 bits
12. **Simultaneous Authentication of Equals** (**SAE**) replaces the PSK; it is more secure as the password is never transmitted, and it is immune to offline attacks
13. Wi-Fi Enhanced Open is the WPA3 equivalent of Open System Authentication; it does not use a password and prevents eavesdropping.
14. This is WAP3 as it has AES encryption up to 256 bit, whereas WPA2 only uses 128-bit encryption.
15. With WPS, you push the button to connect to the wireless network. It is susceptible to a brute-force attack as it has a password stored on the device.
16. A captive portal can ask you to agree to an AUP and provide additional validation, such as your email address or Facebook or Google account details.
17. Wi-Fi Easy Connect makes it very easy to connect IoT devices such as a smartphone by simply using a QR code.
18. A certificate on the endpoint as TLS needs an x509 certificate.
19. They have violated the **Acceptable Use Policy** (**AUP**).
20. If they adopt BYOD, they might have to support hundreds of different devices, whereas if they adopt CYOD, there would be a limited number of devices to make support easier.
21. You could use your cellular phone as a hotspot.
22. If your cell phone is lost or stolen, then you should remote wipe it.

23. You should use screen locks and strong passwords, and use FDE to protect the data at rest.
24. You could tag the laptops and set up geofencing to prevent thefts. RFID is another option.
25. You could segment the data using storage segmentation or containerization.
26. To segment business data and prevent applications outside of the Knox container from accessing resources inside the container.
27. **Near-Field Communication** (**NFC**)

Chapter 9 – Identifying Threats, Attacks, and Vulnerabilities

1. Because you have parted with money, this is a subtle form of ransomware.
2. A fileless virus piggybacks itself onto a legitimate application, and they both launch together. Using Malwarebytes would alert you of both launching at the same time.
3. Credential harvesting is done by a phishing attack where you are warned that an account has been hacked, and it gives you a link to a website to resolve it. That way, when you try to log in, they collect your details.
4. Pretexting is where an attacker manufactures a scenario such as saying that there is suspicious activity on your account, and they ask you to confirm your account details. This way, they can steal them.
5. An attacker obtains the details of a legitimate invoice and sends the company reminders that it needs to be paid, but they substitute the bank details with their own.
6. An attacker works out what standard naming convention a company is using, and they then obtain the names of employees from the internet. They then try common passwords against those accounts.
7. An attacker leaves a malicious USB drive inside a company where it can be found. There is only one shortcut, so when the finder puts it in their computer to try and find the owner, they click on the only visible file and get infected. The attacker can now control their computer.
8. Artificial intelligence uses machine learning to teach the machine to think like a human and detect attacks. So, if it is tainted, it will ignore attacks by the attackers.

9. When you go to a restaurant, please ensure that the server does not disappear with your card; make sure it is always visible to you.
10. An on-path attack is an interception attack, for example, a replay or man-in-the-middle attack.
11. Operational technology is where we have removed CCTV standalone systems that were air-gapped and we now use a fully integrated solution that is fully connected, leaving them vulnerable to attacks.
12. An example of crypto-malware is ransomware where the victim's hard drive is encrypted and held to ransom. It could also have popups.
13. A worm replicates itself and can use either port `4444` or `5000`.
14. A Trojan inserts a `.dll` into either the `SysWOW64` or `System 32` folder.
15. A Remote Access Trojan (RAT) is a Trojan that sends the user's username and password to an external source so that a remote session can be created.
16. A rootkit virus attacks the root in the Windows/`System 32` folder, or in a Bash shell in Linux. For Windows, you may reinstall the OS, but the virus will still be there.
17. A logic bomb virus is triggered by an event; for example, a Fourth of July logic bomb would activate when the date on the computer was July 4. It is triggered by time, scripty, `.bat/.cmd` files, or a task scheduler.
18. A keylogger is a piece of software that could run from a USB flash drive plugged into the back of a computer, which then records all the keystrokes being used. It can capture sensitive data that is typed in, such as bank account details and passwords.
19. A botnet is a group of computers that have been infected so that they can be used to carry out malicious acts without the real attacker being identified. They could be used for a DDoS attack.
20. A phishing attack is when a user receives an email asking them to fill in a form requesting their bank details.
21. Spear phishing is a phishing attack that has been sent to a group of users.
22. A whaling attack targets a CEO or a high-level executive in a company.
23. A vishing attack can use a telephone or leave a voicemail.
24. Social engineering tailgating is where someone has used a smart card or entered a pin to access a door, and then someone behind them passes through the door before it closes, entering no credentials.

25. Social engineering exploits an individual's character in a situation that they are not used to. This is hacking the human, putting them under pressure to make a snap decision.
26. Dressing as a police officer could be part of an impersonation attack.
27. If you let a fireperson into the server room to put out a fire, that is a social engineering urgency attack.
28. If I am using an ATM and someone films the transaction, this is a subtle shoulder surfing attack.
29. Fake software that will not install is a hoax. An email alert telling you to delete a system file as it is a virus is also a hoax.
30. A watering hole attack infects a trusted website that a certain group of people visits regularly.
31. An email that looks like it has come from your company's CEO telling you to carry out an action is a social engineering authority attack.
32. This is a social engineering consensus attack, where the person being attacked wants to be accepted by their peers.
33. An attack with multiple SYN flood attacks is a DDoS attack.
34. A Man-in-the-Middle (MITM) attack is an on-path attack where a connection between hosts is intercepted and the conversation is changed and then replayed, but the people involved still believe that they are talking directly to each other.
35. A reply attack is similar to an MITM attack, except the intercepted packet is replayed at a later date.
36. A POODLE attack is an MITM attack using an SSL3.0 browser that uses Cipher Block Chaining (CBC).
37. A man-in-the-browser attack is a Trojan that intercepts your session between your browser and the internet; it aims to obtain financial transactions.
38. Kerberos authentication uses USN and timestamps and can prevent a replay attack, as the USN packets and the timestamps need to be sequential.
39. Enabling Kerberos or disabling NTLM would prevent a pass-the-hash attack.
40. XSS uses HTML tags with JavaScript.
41. A zero-day virus has no patches and cannot be detected by NIDS or NIPS, as it may take the anti-virus vendor up to 5 days to release a patch.

42. Domain hijacking is where someone tries to register your domain, access your hosted control panel, and set up a website that is similar to yours.
43. Bluejacking is hijacking someone's Bluetooth phone so that you can take control of it and send text messages.
44. Bluesnarfing is when you steal someone's contacts from their Bluetooth phone.
45. An ARP attack is a local attack that can be prevented by using IPSec.
46. `strcpy` can be used for a buffer overflow attack.
47. An integer overflow inserts a number larger than what is allowed.
48. An attack that uses the phrase `1=1` is a SQL injection attack.
49. Input validation and stored procedures can prevent a SQL injection attack. Stored procedures are the best.
50. Session hijacking is where your cookies are stolen so that someone can pretend to be you.
51. Typosquatting is where an attacker launches a website with a similar name to a legitimate website in the hope that victims misspell the URL.
52. Shimming and refactoring are used for driver manipulation attacks.
53. Digital signatures are susceptible to a birthday attack.
54. Rainbow tables are pre-computed lists of passwords with the relevant hash in either MD5 or SHA-1.
55. Salting passwords inserts a random value and prevents dictionary attacks, as a dictionary does not contain random characters.
56. Two tools that can be used for key stretching are bcrypt and PBKDF2.
57. A brute-force attack is the fastest password attack that will crack any password, as it uses all combinations of characters, letters, and symbols.
58. An account locked with a low value is the only way to prevent a brute-force attack.
59. If account lockout is not available, the best way to slow down a brute-force attack is to make the password length longer or to salt passwords.
60. Using passwords for authentication is more prone to errors as certificates and smart cards don't tend to have many errors.
61. An evil twin is a WAP that is made to look like a legitimate WAP.
62. Using an 802.1x authentication switch can prevent an attack by a rogue WAP, as the device needs to authenticate itself to attach to the switch.

63. A wireless disassociation attack is where the attacker prevents the victim from connecting to the WAP.
64. An attacker needs to be within 4 cm of a card to launch an NFC attack.
65. A pivot is where you gain access to a network so that you can launch an attack on a secondary system.

Chapter 10 – Governance, Risk, and Compliance

1. A vulnerability is a weakness that an attacker could exploit.
2. A BPA is used by companies in a joint venture and it lays out each party's contribution, their rights and responsibilities, how decisions are made, and who makes them.
3. A multi-party risk is where someone wins a contract and sub-contracts to a third party who could sabotage your systems.
4. This is where your intellectual property has been stolen, for example, trade secrets, copyright, and patents.
5. A memorandum of understanding is a formal agreement between two parties, but it is not legally binding, whereas a memorandum of agreement is similar, but is legally binding.
6. Tokenization is where data is replaced by a stateless token and the actual data is held in a vault by a payment provider.
7. He has carried out a software licensing compliance violation.
8. An **Interconnection Security Agreement** (**ISA**) states how connections should be made between two business partners. They decide on the type of connection and how to secure it; for example, they may use a VPN to communicate.
9. Shadow IT would connect their own computers to your network without your consent and could lead to pivoting.
10. An inherent risk is a raw risk before it has been mitigated.
11. The four stages of the information life cycle are creation, use, retention, and disposal.
12. They work together so that **Cyber Threat Intelligence** (**CTI**) can be distributed over HTTP.

13. If we adopted separation of duties in the finance department, we would ensure that nobody in the department carried out both parts of a transaction. For example, we would have one person collecting revenue and another person authorizing payments.
14. A risk register lays out all of the risks that a company faces; each risk will have a risk owner who specializes in that area and decides on the risk treatment.
15. Impact assessment is where you evaluate the risk of collecting big data and what tools can be used to mitigate the risk of holding so much data.
16. This is an example of an environmental threat.
17. Job rotation ensures that employees work in all departments so that if someone leaves at short notice or is ill, cover can be provided. It also ensures that any fraud or theft can be detected.
18. A privacy notice gives consent for data only to be collected and used for one specific purpose.
19. This is where data is stored, showing only portions of the data; for example, you might see only the last four digits of a credit card, as follows: `**** **** **** 1234`.
20. They are most likely going to be sued by the customer.
21. It deals with the effectiveness of controls and has limited access as it provides a detailed report about a company.
22. Mandatory vacations ensure that an employee takes at least 5 days of holiday and someone provides cover for them; this also ensures that fraud or theft can be detected.
23. He is measuring BIA as the most important factor to avoid is a single point of failure.
24. The first stage in risk assessment is identifying and classifying an asset. How the asset is treated, accessed, or scored is based on the classification.
25. The Malware Information Sharing Platform provides **Open Source Intelligence** (**OSINT**).
26. This is an example of a functional recovery plan.
27. A clean desk policy is to ensure that no documents containing company data are left unattended overnight.
28. This is a code repository that holds information about malware signatures and code.

29. Someone bringing their own laptop is called BYOD and this is governed by two policies: the onboarding policy and the **Acceptable Use Policy** (**AUP**). The AUP lays out how the laptop can be used, for example, accessing social media sites such as Facebook or Twitter is forbidden while using the device at work.
30. An exit interview is to find out the reason why the employee has decided to leave; it may be the management style or other factors in the company. The information from an exit interview may help the employer improve their working conditions and therefore have a higher retention rate.
31. MITRE ATT&CK is a spreadsheet that shows groups of adversaries, which can be drilled down to see the attack methods and tools used by them.
32. GDPR was developed by the EU to protect an individual's right of privacy.
33. That would be a gray hat hacker as he is provided with limited information.
34. They would use Tor software, The Onion Router, which has thousands of relays to prevent detection.
35. This is training for both red and blue teams where they capture a flag when they achieve each level of training. When they have completed all levels, they are fit to become full-blown red or blue team members.
36. When a risk is deemed too dangerous or high risk and could end in loss of life or financial loss, we would treat the risk with risk avoidance and avoid the activity.
37. Risk transference is where the risk is medium to high and you wish to offload the risk to a third party, for example, insuring your car.
38. Automated Indicator Sharing was invented by the US federal government to exchange data about cyber attacks from the state down to the local level.
39. 27701 was developed as a standard as an extension of 27001/27002 to be used for privacy information management.
40. Rules of behavior are how people should conduct themselves at work to prevent discrimination or bullying.
41. IOC informs members of their IT security community of IP addresses, hashes, or URLs where they have discovered newly released malware.
42. A script kiddie wants to be on the national news and TV as they seek fame.
43. Annual security awareness training advises employees of the risk of using email, the internet, and posting information on social media websites. It also informs employees of any new risks posed since the last training.

44. Sending an email to everyone who works in your company using your Gmail account is a violation of the AUP and could lead to disciplinary action.
45. A manufacturing company would carry out a supply chain risk assessment because they need a reputable supplier of raw materials so that they can manufacture goods.
46. Business impact analysis is just money; it looks at the financial impact following an event. The loss of earnings, the cost of purchasing new equipment, and regulatory fines are calculated.
47. The **Recovery Point Object** (**RPO**) is the acceptable downtime that a company can suffer without causing damage to the company, whereas the **Recovery Time Object** (**RTO**) is the time it takes for the company to return to an operational state – this should be within the RPO.
48. **Mean Time to Repair** (**MTTR**) is the average time it takes to repair a system, but in the exam, it could be seen as the time to repair a system and not the average time.
49. A competitor would seek to damage your production systems and steal your trade secrets.
50. Criminal syndicates would threaten you and demand payment as they are financially driven.
51. **Mean Time Between Failure** (**MTBF**) is the measurement of the reliability of a system.
52. SSAE assists CPA in carrying out the auditing of SOC reports.
53. **Single Loss Expectancy** (**SLE**) is the cost of the loss of one item; if I lose a tablet worth $1,000, then the SLE is $1,000.
54. The **Annual Loss Expectancy** (**ALE**) is calculated by multiplying the SLE by the ARO (the number of losses per year). If I lose six laptops a year worth $1,000 each, the ALE would be $6,000.

Chapter 11 – Managing Application Security

1. Mobile devices can connect through cellular, wireless, and Bluetooth connections.
2. Embedded electronic systems have software embedded into the hardware; some use SoC. Examples are microwave ovens, gaming consoles, security cameras, wearable technology, smart TVs, medical devices, such as defibrillators, or self-driving cars.
3. SCADA systems are industrial control systems used in the refining of uranium, oil, or gas, or the purification of water.

4. Smart TVs and wearable technology are classified as IoT devices.
5. Home automation is where you can control the temperature, lighting, entertainment systems, alarm systems, and many appliances.
6. An SoC is a low-power integrated chip that integrates all of the components of a computer or electronic system. An example would be the controller for a defibrillator. Think of it as an operating system stored on a small chip.
7. The **Real-Time Operating System** (**RTOS**) processes data as it comes in without any buffer delays. The process will fail if it is not carried out within a certain period of time.
8. An attacker would most likely gain control of an MFP through its network interface.
9. When a security team controls the HVAC in a data center, they can ensure that the temperature is regulated and the servers remain available. They also know which rooms are occupied based on the use of air conditioning and electricity.
10. An SoC gives instructions on the steps to take when using a defibrillator; however, if it detects a pulse, it will not send a charge.
11. An example of embedded systems is vehicles that are either self-parking or self-driving.
12. Unmanned aerial vehicles are drones or small, model aircraft that can be sent to areas where manned aircraft cannot go. They can be fitted with a camera to record events or take aerial photographs; an example of these would be to determine the spread of a forest fire.
13. A race condition is when two threads of an application access the same data.
14. The perfect way to set up error handling is for the user to get generic information but for the log files to include a full description of the error.
15. Input validation is where data that is in the correct format is validated prior to being inserted into the system. SQL injection, buffer overflow, and integer overflow are prevented by using input validation.
16. The best way to prevent a SQL injection attack is by using stored procedures.
17. Code signing confirms that the code has not been tampered with.
18. Obfuscation is taking code and masking the data, making it obscure so that if it is stolen, it will not be understood. XOE and ROT13 could be used for obfuscation.

19. Dead code is code that is never used but could introduce errors into the program life cycle; it should be removed.
20. Using a third-party library will help a developer obtain code from the internet to help make an application and get it to market quickly. There are many for Android and JavaScript.
21. The measured boot logs information about the firmware and application and stores this log in the TPM chips. This can be used to check the health status of the host and anti-malware can check during the boot process that the software is trustworthy.
22. UEFI is a modern version of the BIOS and is needed for secure boot.
23. Checking the integrity of the software as it is being loaded is known as attestation.
24. It is a centralized console that continuously monitors the computer and makes automatic alerts when a threat has been detected. It uses machine learning.
25. Fingerprinting is the deep analysis of a host.
26. An NGFW has the ability to act as a stateful firewall by carrying out deep packet filtering.
27. Tokenization takes sensitive data, such as a credit card number, and replaces it with random data, so it cannot be reversed. Encryption can be reversed.
28. We can set the secure flag on the website to ensure that cookies are only downloaded when there is a secure HTTPS session.
29. HSTS ensures that the web browser only accepts secure connections and prevents XSS.
30. They will use dynamic code analysis so that they can use fuzzing to test the code.
31. The Docker tool allows you to isolate applications into a separate space called containers. The registry can now be isolated in a separate container, making it more secure.
32. Opal is a self-encrypting drive where the encryption keys are stored on the hard drive controller and are therefore immune to a cold boot attack and are compatible with all operating systems. They do not have the vulnerabilities of software-based encryption. As a hardware solution, they outperform software solutions.
33. Quality assurance is completed during the staging environment where users test the new application with real data.

Chapter 12 – Dealing with Incident Response Procedures

1. RAID 5 has a minimum of three disks and you can afford to lose one disk without losing data.
2. RAID 6 has a minimum of four disks.
3. RAID 5 has single parity and can lose one disk, whereas RAID 6 has double parity and can lose two disks.
4. A diskless virtual host will get its disk space from an SAN.
5. An SAN will use fast disks, such as SSDs.
6. Cloud storage for personal users could be iCloud, Google Drive, Microsoft OneDrive, or Dropbox.
7. Eradication is where we remove viruses and reduce the services being used. It should be isolated, and this is the containment phase. The virus would be removed in the eradication phase, and then be placed back online. This is the recovery phase.
8. A simulation is where the IRP team is given a specific scenario to deal with.
9. This is an aid to help prepare your business against different adversaries. You can drill down from an adversary into the tactics and techniques that they use. You can then take mitigation steps to avoid being attacked.
10. The four key elements are adversary, capabilities, infrastructure, and victims.
11. If they understand their roles and responsibilities, it can make them more effective when a disaster happens.
12. The contents of memory are saved in a dump file and this can be used to investigate the event.
13. It gives you clear visibility of network traffic patterns and can identify malicious traffic.
14. An HTTP status code of `200 OK` lets you know that a successful connection has been made.
15. Playbooks contain a set of rules to enable the SOAR to take preventative action as an event occurs.
16. It can help load balance the network traffic and provide redundancy if one card fails.

17. The UPS is basically a battery that is a standby device so that when the computer power fails, it kicks in. It is designed to keep the system going for a few minutes to allow the server team to close the servers down gracefully. It can also be used to clean up the power coming from the National Grid, such as spikes, surges, and voltage fluctuations.
18. Two **Host Bus Adapters** (**HBAs**) on each node will give two separate paths to them.
19. This would be diversity, so that if one vendor had a disaster, the other would keep providing the broadband.
20. An incident response plan is written for a particular incident and lays out how it should be tackled and the key personnel required.
21. The different categories of incidents are as follows:

    a. Unauthorized access

    b. Loss of computers or data

    c. Loss of availability

    d. Malware attack

    e. DDoS attack

    f. Power failure

    g. Natural disasters, such as floods, tornadoes, hurricanes, and fires

    h. Cybersecurity incidents
22. The different roles required to deal with an incident are as follows:

    a. **Incident response manager**: A top-level manager takes charge.

    b. **Security analyst**: Provides technical support for the incident.

    c. **IT auditor**: Checks that the company is compliant.

    d. **Risk analyst**: Evaluates all aspects of risk.

    e. **HR**: Sometimes, employees are involved in the incident.

    f. **Legal**: Gives advice and makes decisions on legal issues.

    g. **Public relations**: Deals with the press to reduce the impact on the company's reputation.
23. The help desk identifies the incident response plan required and the key personnel that need to be notified.

24. An incident response exercise is for carrying out the incident response plan and planning for any shortfalls.
25. The first phase of the incident response process is the preparation phase, where the plan is already written in advance of any attack.
26. The last phase of the incident response process is lessons learned, where we review why the incident was successful.
27. If we do not carry out lessons learned, the incident may re-occur. Lessons learned is a detective control where we try to identify and address any weaknesses.
28. This is where we isolate or quarantine an infected machine.
29. This is where we remove malware and turn off services that we do not need.
30. This is where we put infected machines back online, restore data or reimage desktops.