1.1
1. What are the properties of a secure information processing system?

- Confidentiality, Integrity, and Availability (and Non-remediation).
- Confidentiality, Integrity, and Availability (and Non-repudiation).
- Confidentiality, Identity, and Availability (and Non-repudiation).
- Concentration, Integrity, and Availability (and Non-repudiation).

2. What term is used to describe the property of a secure network where a sender cannot deny having sent a message?

- Non-Repudiation
- Non-Remediation
- Non-Reunification

3. A multinational company manages a large amount of valuable intellectual property (IP) data, plus personal data for its customers and account holders. What type of business unit can be used to manage such important and complex security requirements?

- SOK
- SOC
- SOG
- SOB

4. A business is expanding rapidly and the owner is worried about tensions between its established IT and programming divisions. What type of security business unit or function could help to resolve these issues?

- DevUps
- NevUps
- DevOps
- NevOps

5. You have implemented a secure web gateway that blocks access to a social networking site. How would you categorize this type of security control?

- It is a technical type of control (implemented in software) and acts as a primary measure.
- It is a technical type of control (implemented in software) and acts as a preservative measure.
- It is a technical type of control (implemented in software) and acts as a preventative measure.
- It is a technical type of control (implemented in software) and acts as a preemptive measure.

6. A company has installed motion-activated floodlighting on the grounds around its premises. What class and function(s) is this security control?

- It is a physical control and its function is both to detect and deter.
- It is a logical control and its function is both to disable and undermine.
- It is a physical control and its function is both to monitor and alert.
- It is a logical control and its function is both to undermine and deter.

7. A firewall appliance intercepts a packet that violates policy. It automatically updates its Access Control List to block all further packets from the source IP. What TWO functions is the security control performing?

- Protective and curative
- Preventative and corrective
- Persuasive and control

8. If a security control is described as operational and compensating, what can you determine about its nature and function?

- That the control is enforced by a person rather than a technical system, and that the control has been developed to replicate the functionality of a primary control, as required by a security standard.
- That the control is enforced by a system rather than a person, and that the control has been developed to replicate the functionality of a primary control, as required by a security standard.
- That the control is enforced by a person rather than a technical system, and that the control has been developed to replicate the functionality of a tertiary control, as required by a security standard.
- That the control is enforced by a person rather than a technical system, and that the control has been developed to replicate the functionality of a secondary control, as required by a security standard.

9. Which of the following would be assessed by likelihood and impact?

- vulnerability
- threat
- risk
- weakness

10. Nation state actors primarily only pose a risk to other states. False—nation state actors have targeted commercial interests for theft, espionage, and extortion.

- True—nation state actors only attack other nation states.
- False—nation state actors have targeted commercial interests for theft, espionage, and extortion.

1.2

1. You suspect that a rogue host is acting as the default gateway for a subnet in a spoofing attack. What command-line tool(s) can you use from a Windows client PC in the same subnet to check the interface properties of the default gateway?

- IPCONFIG, ARP, ROUTE
- IPCONFIG, PINGPATH, ROUTE
- IFCONFIG, ARP, ROUTE
- IFCONFIG, PINGPATH, ARP

2. You suspect the rogue host is modifying traffic before forwarding it, with the side effect of increasing network latency. Which tool could you use to measure latency on traffic routed from this subnet?

- ROUTE
- PINGPATH
- DIG
- IPCONFIG

3. What type of tool could you use to fingerprint the host acting as the default gateway?

- NMAP

- DIG
- IPCONFIG
- NETSTAT

4. You are investigating a Linux server that is the source of suspicious network traffic. At a terminal on the server, which tool could you use to check which process is using a given TCP port?

- NMAP
- DIG
- IPCONFIG
- NETSTAT

5. What is a zone transfer and which reconnaissance tools can be used to test whether a server will allow one?

- NMAP
- DIG
- IPCONFIG
- NETSTAT

6. You are developing new detection rules for a network security scanner. Which tool will be of use in testing whether the rules match a malicious traffic sample successfully?

- TCPREPLAY
- NSLOOKUP
- DNSFLUSH
- DNSENUM

7. What type of organizational security assessment is performed using Nessus?

- network vulnerability scanning
- remote access scanning
- SSH client scanning
- social engineering scanning

8. What security posture assessment could a pen tester make using Netcat?

- Whether it is possible to open a network connection to a remote host over an unknown port.
- Whether it is possible to open a network connection to a localhost over a given port.
- Whether it is possible to open a network connection to a remote host over a given port.
- Whether it is possible to open a network connection to a localhost over an unknown port.

9. You are recommending that a business owner invest in patch management controls for PCs and laptops. What is the main risk from weak patch management procedures on such devices?

- Vulnerabilities in the OS and applications software such as web browsers and document readers or in PC and adapter firmware can allow threat actors to run malware and gain complete control of the network.
- Vulnerabilities in the OS and applications software such as web browsers and document readers or in PC and adapter firmware can prevent threat actors from running malware and gain a foothold on the network.
- Vulnerabilities in the OS and applications software such as web browsers and document readers or in PC and adapter firmware can allow compliance professionals to run malware and gain a foothold on the network.
- Vulnerabilities in the OS and applications software such as web browsers and document readers or in PC and adapter firmware can allow threat actors to run malware and gain a foothold on the network.

10. You are advising a business owner on security for a PC running Windows XP. The PC runs process management software that the owner cannot run on Windows 10. What are the risks arising from this, and how can they be mitigated?

- Windows XP is a actively supported platform that is no longer receiving security updates. This means that patch management cannot be used to reduce risks from software vulnerabilities. The workstation should be isolated from other systems to reduce the risk of compromise.
- Windows XP is a actively supported platform that is still receiving security updates. This means that patch management cannot be used to reduce risks from software vulnerabilities. The workstation should be isolated from other systems to reduce the risk of compromise.
- Windows XP is a actively supported platform that is no longer receiving security updates. This means that patch management cannot be used to reduce risks from software vulnerabilities. The workstation should be isolated from other systems to reduce the risk of compromise.

- Windows XP is a legacy platform that is no longer receiving security updates. This means that patch management cannot be used to reduce risks from software vulnerabilities. The workstation should be isolated from other systems to reduce the risk of compromise.

11. Mitigating risks of data breach requires effective secure processing, authorization, and authentication security controls.

- True
- False

12. A system integrator is offering a turnkey solution for customer contact data storage and engagement analytics using several cloud services. Does this solution present any supply chain risks beyond those of the system integrator's consulting company?

- Yes, the system integrator is proposing the use of multiple vendors (the cloud service providers), with potentially complex issues for collecting, storing, and sharing customer personal data across these vendors. Each company in the supply chain should be assessed for risk and compliance with cybersecurity and privacy standards.
- No, the system integrator is proposing the use of multiple vendors (the cloud service providers), with potentially complex issues for collecting, storing, and sharing customer personal data across these vendors. Each company in the supply chain should be assessed for risk and compliance with cybersecurity and privacy standards.
- It depends. The system integrator is proposing the use of multiple vendors (the cloud service providers), with potentially complex issues for collecting, storing, and sharing customer personal data across these vendors. Each company in the supply chain should be assessed for risk and compliance with cybersecurity and privacy standards.
- Cloud services are always reliable, so no. The system integrator is proposing the use of multiple vendors (the cloud service providers), with potentially complex issues for collecting, storing, and sharing customer personal data across these vendors. Each company in the supply chain should be assessed for risk and compliance with cybersecurity and privacy standards.

13. You have configured a network vulnerability scanner for an engineering company. When running a scan, multiple sensors within an embedded systems network became unresponsive, causing a production shutdown. What alternative method of vulnerability scanning should be used for the embedded systems network?

- Packet Sniffing
- Automated OS Patching
- Pen Testing
- CVE scanning

1.3

1. The help desk takes a call and the caller states that she cannot connect to the e-commerce website to check her order status. She would also like a user name and password. The user gives a valid customer company name but is not listed as a contact in the customer database. The user does not know the correct company code or customer ID. Is this likely to be a social engineering attempt, or is it a false alarm?

- It is social engineering.
- It is a false alarm.
- It is a false positive.
- It is neither. It is just a human oversight.

2. A purchasing manager is browsing a list of products on a vendor's website when a window opens claiming that anti-malware software has detected several thousand files on his computer that are infected with viruses. Instructions in the official-looking window indicate the user should click a link to install software that will remove these infections. What type of social engineering attempt is this, or is it a false alarm?

- This is a social engineering attempt utilizing a honeypot and/or malvertising.
- This is a social engineering attempt utilizing a honeynet and/or malvertising.
- This is a social engineering attempt utilizing a watering hole and/or malvertising.
- This is a social engineering attempt utilizing a MITM and/or malvertising.

3. Your CEO calls to request market research data immediately be forwarded to her personal email address. You recognize her voice, but a proper request form has not been filled out and use of third-party email is prohibited. She states that normally she would fill out the form and should not be an exception, but she urgently needs the data to prepare for a round table at a conference she is attending. What type of social engineering techniques could this use, or is it a false alarm?

- If it is social engineering, then this is not spear phishing (the attack uses specific detail) over a voice channel (vishing). It is possible that it uses deep fake technology for voice mimicry. The use of a sophisticated attack for a relatively low-value data asset seems unlikely, however. A fairly safe approach would be to contact the CEO back on a known mobile number.
- If it is social engineering, then this is whaling or spear phishing (the attack uses specific detail) over a voice channel (vishing). It is not yet possible that it uses deep fake technology for voice mimicry. The use of a sophisticated attack for a relatively low-value data asset seems unlikely, however. A fairly safe approach would be to contact the CEO back on a known mobile number.
- If it is social engineering, then this is whaling or spear phishing (the attack uses specific detail) over a voice channel (vishing). It is possible that it uses deep fake technology for voice

mimicry. The use of a sophisticated attack for a relatively low-value data asset seems unlikely, however. do not contact the CEO back on a known mobile number in order to confirm identity.

- If it is social engineering, then this is whaling or spear phishing (the attack uses specific detail) over a voice channel (vishing). It is possible that it uses deep fake technology for voice mimicry. The use of a sophisticated attack for a relatively low-value data asset seems unlikely, however. A fairly safe approach would be to contact the CEO back on a known mobile number.

4. Your company manages marketing data and private information for many high-profile clients. You are hosting an open day for prospective employees. With the possibility of social engineering attacks in mind, what precautions should employees take when the guests are being shown around the office?

- Employees should specifically be wary of shoulder surfing attempts to observe passwords and the like.
- Employees should specifically be wary of spear phishing attempts to observe passwords and the like.
- Employees should specifically be wary of lunchtime attacks to find passwords and the like.
- Employees should specifically be wary of shoulder surfing attempts to lure employees to follow an email link.

5. Employees should specifically be wary of shoulder surfing attempts to observe passwords and the like.

- This is some type of phishing scheme, but it will take more investigation whether it is actually crypto-malware or not.
- This is some type of ransomware, and you can assume that it is actually crypto-malware.
- This is some type of ransomware, but it will take more investigation whether it is actually crypto-malware or not.
- This is some type of ransomware, but it will take more investigation whether it is actually cryptography or not.

6. You are writing a security awareness blog for company CEOs subscribed to your threat platform. Why are backdoors and Trojans different ways of classifying and identifying malware risks?

- A Trojan means a malicious program masquerading as something else; a backdoor is a covert means of accessing a host or network. A Trojan need not necessarily operate a backdoor and a backdoor can be established by exploits other than using Trojans. The term remote access trojan (RAT) is a general term for for Trojan and backdoor.
- A Trojan means a malicious program masquerading as something else; a backdoor is a covert means of accessing a host or network. A Trojan need not necessarily operate a backdoor

and a backdoor can be established by exploits other than using Trojans. The term remote access trojan (RAT) is used for the specific combination of Trojan and backdoor.

- A Trojan means a malicious program masquerading as something else; a backdoor is a covert means of accessing a host or network. A Trojan by definition operates a backdoor and a backdoor will be established by exploits other than using Trojans. The term remote access trojan (RAT) is used for the specific combination of Trojan and backdoor.
- A Trojan is an innocent program masquerading as malware; a backdoor is a covert means of accessing a host or network. A Trojan need not necessarily operate a backdoor and a backdoor can be established by exploits other than using Trojans. The term remote access trojan (RAT) is used for the specific combination of Trojan and backdoor.

7. You are investigating a business email compromise (BEC) incident. The email account of a developer has been accessed remotely over webmail. Investigating the developer's workstation finds no indication of a malicious process, but you do locate an unknown USB extension device attached to one of the rear ports. Is this the most likely attack vector, and what type of malware would it implement?

- It is likely that the USB device is used for storage. This would not necessarily require any malware to be installed or leave any trace in the file system.
- It is likely that the USB device implements a hardware-based keylogger. This would require malware to be installed or leave traces in the file system.
- It is likely that the USB device implements a hardware-based keylogger. This would not necessarily require any malware to be installed but it would leave records and fingerprints in the file system.
- It is likely that the USB device implements a hardware-based keylogger. This would not necessarily require any malware to be installed or leave any trace in the file system.

8. A user's computer is performing extremely slowly. Upon investigating, you find that a process named notepad.exe is utilizing the CPU at rates of 80-90%. This is accompanied by continual small disk reads and writes to a temporary folder. Should you suspect malware infection and is any particular class of indicated?

- No, this is not malware as the process name is not masquerading as a legitimate process. It is possible to conclusively determine the type without more investigation, but you might initially suspect the computer might be being used for a DDoS attack
- No, this is not malware as the process name is not masquerading as a legitimate process. It is possible to conclusively determine the type without more investigation, but you might initially suspect a crypto-miner/crypto-jacker.
- Yes, this is malware as the process name is not trying to masquerade as a legitimate process. It is not possible to conclusively determine the type without more investigation, but you might initially suspect a crypto-miner/crypto-jacker.

- Yes, this is malware as the process name is trying to masquerade as a legitimate process. It is not possible to conclusively determine the type without more investigation, but you might initially suspect a crypto-miner/crypto-jacker.

9. Which part of a simple cryptographic system must be kept secret

- Cipher
- Algorithm
- Ciphertext
- Private Key
- Public Key

10. Considering that cryptographic hashing is one-way and the digest cannot be reversed, what makes hashing a useful security technique?

- Because two parties can hash the same data and compare checksums to see if they match, hashing can be used for data verification in a variety of situations, including password authentication. Hashes of passwords, rather than the password plaintext, can be stored securely or exchanged for authentication. A hash of a file or a hash code in an electronic message can be verified by both parties.
- Because two parties can hash the same data and compare checksums to see if they match, hashing can be used for data verification in a variety of situations, including password authentication. Hashes of passwords, rather than the password plaintext, can not be stored securely or exchanged for authentication. A hash of a file or a hash code in an electronic message can be verified by both parties.
- Because two parties can hash the same data and compare checksums to see if they match, hashing can not be used for data verification in a variety of situations, including password authentication. Hashes of passwords, rather than the password plaintext, can be stored securely or exchanged for authentication. A hash of a file or a hash code in an electronic message can be verified by both parties.
- Because two parties can not hash the same data and compare checksums to see if they match, hashing can be used for data verification in a variety of situations, including password authentication. Hashes of passwords, rather than the password plaintext, can be stored securely or exchanged for authentication. A hash of a file or a hash code in an electronic message can be verified by both parties.

11. What is the process of digitally signing a message?

- A hashing function is used to create a message digest. The digest is then signed using the sender's private key. The resulting signature can be decrypted by the recipient using the

sender's public key and cannot be modified by any other agency. The recipient can calculate his or her own digest of the message and compare it to the signed hash to validate that the message has not been altered.

- A hashing function is used to create a message digest. The digest is then signed using the sender's private key. The resulting signature can be decrypted by the recipient using the sender's public key and cannot be modified by any other agency. The recipient can not calculate his or her own digest of the message and compare it to the signed hash to validate that the message has not been altered.
- A hashing function is used to create a message digest. The digest is then signed using the sender's private key. The recipient can calculate his or her own digest of the message and compare it to the signed hash to validate that the message has not been altered.
- A hashing function is used to create a message digest. The resulting signature can be decrypted by the recipient using the sender's public key and cannot be modified by any other agency. The recipient can calculate his or her own digest of the message and compare it to the signed hash to validate that the message has not been altered.

12. True or False? Perfect forward secrecy (PFS) ensures that a compromise of a server's private key will not also put copies of traffic sent to that server in the past at risk of decryption.

- True
- False

13. Cryptography is about keeping things secret so they cannot be used as the basis of a non-repudiation system.

- True
- False

1.4

1. What is the main weakness of a hierarchical trust model?

- The structure does not rely on the integrity of the root DA.
- The structure depends on the integrity of the root CA.
- The structure depends on the integrity of the root BA.
- The structure does not rely on the integrity of the root AA.

2. How does a subject go about obtaining a certificate from a CA?

- In most cases, the subject generates a key pair then adds the public key along with subject information and certificate type in a certificate signing request (CSR) and submits it to the CA. If the CA accepts the request, it generates a certificate with the appropriate key usage and validity, signs it, and transmits it to the subject.
- In most cases, the subject generates a key pair then adds the public key along with subject information and certificate type in a certificate signing request (CSR) and submits it to the CA. If the CA does not accept the request, it generates a certificate with the appropriate key usage and validity, signs it, and transmits it to the subject.
- In most cases, the subject generates a key pair then adds the public key along with subject information and certificate type in a certificate signing request (CSR) and submits it to the CA. If the CA accepts the request, it creates the certificate with the appropriate key usage and validity, signs it, and stores it in escrow.
- In most cases, the CA generates a key pair then adds the public key along with subject information and certificate type in a certificate signing request (CSR) and submits it to the subject. If the Subject accepts the request, it generates a certificate with the appropriate key usage and validity, signs it, and transmits it to the CA.

3. What cryptographic information is stored in a digital certificate?

- The subject's public key and the algorithms used for encryption and hashing. The certificate also stores a digital signature from the issuing CA, establishing the chain of trust.
- The subject's private key and the algorithms used for encryption and hashing. The certificate also stores a digital signature from the issuing KDC, establishing the chain of trust.
- The subject's public key and the algorithms used for encryption and hashing. The certificate also stores a digital signature from the issuing AS, establishing the chain of trust.
- The subject's public key and the algorithms used for encryption and hashing. The certificate also stores a digital signature from the issuing TGS, establishing the chain of trust.

4. What does it mean if a certificate extension attribute is marked as critical?

- That the application processing the certificate must be able to interpret the extension correctly. Otherwise, it will reject the certificate.
- That the server processing the certificate must be able to interpret the extension correctly. Otherwise, it should reject the certificate.
- That the application processing the certificate must be able to interpret the extension correctly. Otherwise, it should reject the certificate.
- That the application processing the digital signature must be able to interpret the extension correctly. Otherwise, it should reject the certificate.

5. You are developing a secure web application. What sort of certificate should you request to show that you are the publisher of a program?

- A code signing certificate. Certificates are issued for many purposes. A certificate issued for one purpose should be reused for other functions.
- A code signing certificate. Certificates are issued for specific purposes. A certificate issued for one purpose should not be reused for other functions.
- A digital certificate. Certificates are issued for many purposes. A certificate issued for one purpose should be reused for other functions.
- A digital certificate. Certificates are issued for many purposes. A certificate issued for one purpose writing code and not for anything else.

6. What extension field is used with a web server certificate to support the identification of the server by multiple specific subdomain labels?

- The subject alternative name (SAN) field. A wildcard certificate will match any subdomain label.
- The subject alternative name (SAN) field. A wildcard certificate will match any domain label.
- The subject alternative name (SAN) field. A wildcard certificate will match any subfolder label.
- The subject alternative name (SAN) field. A wildcard certificate will match any submission.

7. What are the potential consequences if a company loses control of a private key?

- It puts both data confidentiality and identification and authorization systems at risk. Depending on the key usage, the key may be used to decrypt data with authorization. The key could also be used to impersonate a user or computer account.
- It puts both data confidentiality and identification and authentication systems at risk. Depending on the key usage, the key may be used to decrypt data with authorization. The key could also be used to impersonate a user or computer account.
- It puts both data confidentiality and identification and authentication systems at risk. Depending on the key usage, the key may be used to encrypt data with authorization. The key could also be used to impersonate a user or computer account.
- It puts both data confidentiality and identification and authentication systems at risk. Depending on the key usage, the key may be used to decrypt data without authorization. The key could also be used to impersonate a user or computer account.

8. You are advising a customer about encryption for data backup security and the key escrow services that you offer. How should you explain the risks of key escrow and potential mitigations?

- Escrow refers to archiving the key used to encrypt the customer's backups with your company as a third party. The risk is that an insider attack from your company may be able to decrypt the data backups. This risk can be mitigated by requiring M-of-N access to the escrow keys, eliminating the risk of a rogue administrator.
- Escrow refers to archiving the key used to encrypt the customer's backups with your company as a third party. The risk is that an outside threat attack from your company may be able to decrypt the data backups. This risk can be mitigated by requiring M-of-N access to the escrow keys, reducing the risk of a rogue administrator.
- Escrow refers to archiving the key used to encrypt the customer's backups with your company as a third party. The risk is that an insider attack from your company may be able to encrypt the data backups. This risk can be mitigated by requiring M-of-N access to the escrow keys, reducing the risk of a rogue administrator.
- Escrow refers to archiving the key used to encrypt the customer's backups with your company as a third party. The risk is that an insider attack from your company may be able to decrypt the data backups. This risk can be mitigated by requiring M-of-N access to the escrow keys, reducing the risk of a rogue administrator.

9. What mechanism informs clients about suspended or revoked keys?

- Either a published Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) transmitter.
- Either a published Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) responder.
- Either a published Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) sounder.
- Either a published Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) sensor.

10. What mechanism does HPKP implement?

- HTTP Public Key Protocol (HPKP) ensures that when a client inspects the certificate presented by a server or a code-signed application, it is inspecting the proper certificate by submitting one or more public keys to an HTTP browser via an HTTP header.
- HTTP Public Kerberos Protocol (HPKP) ensures that when a client inspects the certificate presented by a server or a code-signed application, it is inspecting the proper certificate by submitting one or more public keys to an HTTP browser via an HTTP header.
- HTTP Public Key Pinning (HPKP) ensures that when a client inspects the certificate presented by a server or a code-signed application, it is inspecting the proper certificate by submitting one or more public keys to an HTTP browser via an HTTP header.

- HTTP Private Key Pinning (HPKP) ensures that when a client inspects the certificate presented by a server or a code-signed application, it is inspecting the proper certificate by submitting one or more public keys to an HTTP browser via an HTTP header.

11. What type of certificate format can be used if you want to transfer your private key and certificate from one Windows host computer to another?

- PKCS #12 / .PFX / .P1.2
- PCKS #12 / .PFX / .P12
- PKCS #12 / .PFX / .P12.
- PKCS #12 / .PPX / .P12

12. What type of operation is being performed by the following command? openssl req -nodes -new -newkey rsa:2048 -out my.csr-keyout mykey.pem

- This generates a new AES key pair plus a certificate signing request.
- This generates a new RSA key pair plus a certificate signing request.
- This generates a new RSA key pair plus a digitally signed certificate.
- This generates a new AES key pair plus a digitally signed certificate.

13. What is the difference between authorization and authentication?

- Authorization means granting the account that has been configured for the user on the computer system the right to make use of a resource. Authorization manages the privileges granted to the user. Authentication protects the validity of the user account by testing that the person accessing that account is who she/he says she/he is.
- Authentication means granting the account that has been configured for the user on the computer system the right to make use of a resource. Authorization manages the privileges granted to the user. Authorization protects the validity of the user account by testing that the person accessing that account is who she/he says she/he is.
- Authorization means granting the account that has been configured for the user on the computer system the right to make use of a resource. Authorization manages the privileges granted on the resource. Authentication protects the validity of the user account by testing that the person accessing that account is who she/he says she/he is.
- Authentication means granting the account that has been configured for the user on the computer system the right to make use of a resource. Authorization manages the privileges granted on the resource. Authorization protects the validity of the user account by testing that the person accessing that account is who she/he says she/he is.

14. What steps should be taken to enroll a new employee on a domain network?

- Perform checks to confirm the user's identity, issue authorization credentials securely, assign appropriate permissions/privileges to the account, and ensure accounting mechanisms to audit the user's activity.
- Perform checks to confirm the user's identity, issue authentication credentials securely, assign appropriate permissions/privileges to the account, and ensure accounting mechanisms to audit the user's activity.
- Perform checks to confirm the user's identity, issue authentication credentials securely, assign appropriate permissions/privileges to the user, and ensure accounting mechanisms to audit the user's activity.
- Perform checks to confirm the user's identity, issue authentication credentials securely, assign appropriate permissions/privileges to the account, and ensure accounting mechanisms to audit the the account's activity.

15. True or false? An account requiring a password, PIN, and smart card is an example of three-factor authentication.

- False—Three-factor authentication also includes a biometric-, behavioral-, or location based element. The password and PIN elements are the same factor (something you know).
- True—Three-factor authentication also includes a biometric-, behavioral-, or location based element. The password and PIN elements are not the same factor (something you know).

16. True or False: You can query the location service running on a device or geolocation by IP. You could use location with the network, based on switch port, wireless network name, virtual LAN (VLAN), or IP subnet.

- True
- False

17. Why might a PIN be a particularly weak type of something you know authentication?

- A long personal identification number (PIN) is difficult for users to remember. Always use a short PIN so the user will remember and use it. A PIN can only be used safely where the number of sequential authentication attempts can be strictly limited.
- A long personal identification number (PIN) is difficult for users to remember, but a short PIN is easy to crack. A PIN can only be used safely where the number of sequential authentication attempts can be strictly limited.

- A long personal identification number (PIN) is difficult for users to remember, but a short PIN is easy to crack. A PIN can only be used safely where the number of sequential authentication attempts can be unlimited.
- A long personal identification number (PIN) is difficult for users to remember. Always use a short PIN so the user will remember and use it. A PIN should not be used if the number of sequential authentication attempts can be strictly limited.

18. In what scenario would PAP be considered a secure authentication method?

- PAP is a actively used protocol that cannot be considered secure because it transmits cipher text ASCII passwords and has no cryptographic protection. The only way to ensure the security of PAP is to ensure that the endpoints established a secure tunnel (using IPSec, for instance).
- PAP is a actively used protocol that can be considered secure because it transmits plaintext ASCII passwords and has no cryptographic protection. The only way to ensure the security of PAP is to ensure that the endpoints established a secure tunnel (using IPSec, for instance).
- PAP is a legacy protocol that can be considered secure because it transmits ciphertext ASCII passwords and has no cryptographic protection. The only way to ensure the security of PAP is to ensure that the endpoints established a secure tunnel (using IPSec, for instance).
- PAP is a legacy protocol that cannot be considered secure because it transmits plaintext ASCII passwords and has no cryptographic protection. The only way to ensure the security of PAP is to ensure that the endpoints established a secure tunnel (using IPSec, for instance).

19. True or false? In order to create a service ticket, Kerberos passes the user's password to the target application server for authentication.

- True
- False

20. A user maintains a list of commonly used passwords in a file located deep within the computer's directory structure. Is this secure password management?

- No. This is security by obscurity. The file could probably be easily discovered using search tools.
- Yes. There is no way possible to find those passwords.

21. Which property of a plaintext password is most effective at defeating a brute-force attack?

- Complexity

- (•) Length
- ( ) Retirement
- ( ) Language

22. True or false? When implementing smart card logon, the user's private key is stored on the smart card.

- (•) True
- ( ) False

1.5

1. Steganography and Code Obfuscation illustrate the security through obscurity concept.

- (•) True
- ( ) False

2. Which of the answers listed below refers to a solution designed to strengthen the security of session keys?

- ( ) ECB
- (•) PFS
- ( ) EFS
- ( ) PFX

3. What is the difference between authorization and authentication?

- ( ) Authentication means granting the account that has been configured for the user on the computer system the right to make use of a resource. Authentication manages the privileges granted on the resource. Authorization protects the validity of the user account by testing that the person accessing that account is who she/he says she/he is.
- (•) Authorization means granting the account that has been configured for the user on the computer system the right to make use of a resource. Authorization manages the privileges granted on the resource. Authentication protects the validity of the user account by testing that the person accessing that account is who she/he says she/he is.
- ( ) Authorization means restricting the account that has been configured for the user on the computer system the right to make use of a resource. Authorization manages the privileges

granted on the user. Authentication protects the validity of the user account by testing that the person accessing that account is not who she/he says she/he is.

- Authorization means restricting the account that has been configured for the user on the computer system the right to make use of a resource. Authorization manages the privileges granted on the author. Authentication protects the validity of the user account by testing that the person accessing that account is who she/he says she/he is.

4. In cryptography, the term "Key stretching" refers to a mechanism for extending the length of a cryptographic key to make it more secure against brute-force attacks.

- True
- False

5. Which of the three states of digital data requires data to be processed in an unencrypted form?

- Data-in-transit
- Data-aqt-rest
- Data-in-use
- Data-in-sync

6. What steps should be taken to enroll a new employee on a domain network?

- Perform checks to confirm the user's identity, issue authentication credentials securely, assign appropriate permissions/privileges to the account, and ensure accounting mechanisms to audit the user's activity.
- Perform checks to confirm the user's identity, issue authorization credentials securely, assign appropriate permissions/privileges to the account, and ensure accounting mechanisms to audit the user's activity.
- Perform checks to confirm the user's identity, issue authentication credentials securely, assign appropriate restrictions to the account, and ensure accounting mechanisms to audit the user's activity.
- Perform checks to confirm the user's identity, issue authentication credentials securely, assign appropriate restrictions to the account, and ensure accounting mechanisms to audit the user's history.

7. An account requiring a password, PIN, and smart card is an example of three-factor authentication.

- True

- False

8. In cryptography, the term "Secret algorithm" refers to an algorithm designed in a way that prevents the examination of its inner workings.

- True
- False

9. The term "Ephemeral key" refers to an asymmetric encryption key designed to be used only for the duration of a single session or transaction.

- True
- False

10. In cryptography, the number of bits in a key used by a cryptographic algorithm is referred to as a key size or key length. The key size determines the maximum number of combinations required to break the encryption algorithm, therefore typically a longer key means stronger cryptographic security.

- True
- False

11. Unlike stream ciphers which process data by encrypting individual bits, block ciphers divide data into separate fragments and encrypt each fragment separately.

- True
- False

12. Which of the following terms is used in conjunction with the assumption that the output of a cryptographic function should be considerably different from the corresponding plaintext input?

- Confusion
- Obfuscation
- Collision
- Diffusion

13. Pseudo-random data used in combination with a secret key in WEP and SSL encryption schemes is known as:

- Salt
- Shim
- IV
- Seed

14. Which of the following answers refers to a type of additional input that increases password complexity and provides better protection against brute-force, dictionary, and rainbow table attacks?

- Seed
- IV
- Salt
- Shim

2.1

1. You are consulting with a company about a new approach to authenticating users. You suggest there could be cost savings and better support for multifactor authentication (MFA) if your employees create accounts with a cloud provider. That allows the company's staff to focus on authorizations and privilege management. What type of service is the cloud vendor performing?

- The company is acting as the identity provider.
- The cloud vendor is acting as the identity protector.
- The cloud vendor is acting as the identity provider.
- The cloud company is acting as the identity protector.

2. What is the process of ensuring accounts are only created for valid users, only assigned the appropriate privileges, and that the account credentials are known only to the valid user?

- Offboarding.
- Onboarding.
- Nearboarding.
- Outboarding.

3. What is the policy that states users should be allocated the minimum sufficient permissions?

- ○ Most privilege.
- ○ Privilege management.
- ○ Privilege minimalization.
- ◉ Least privilege.

4. A standard operating procedure (SOP) is a step-by-step listing of the actions that must be completed for any given task.

- ◉ True
- ○ False

5. What type of organizational policies ensure that at least two people have oversight of a critical business process?

- ○ singular authority, job rotation, and mandatory enforced vacation/holidays.
- ◉ Shared authority, job rotation, and mandatory enforced vacation/holidays.
- ○ Shared authority, job rotation, and voluntary vacation/holidays.
- ○ Singular authority, job rotation, and voluntary vacation/holidays.

6. Recently, attackers were able to compromise the account of a user whose employment had been terminated a week earlier. They used this account to access a network share and delete important files. What account vulnerability enabled this attack?

- ○ While it's possible that strict password requirements and incorrect privileges may have contributed to the account compromise, the most glaring problem is that the terminated employee's account wasn't disabled. Since the account was no longer being used
- ○ While it's possible that lax password requirements and correct privileges may have contributed to the account compromise, the most glaring problem is that the terminated employee's account wasn't disabled. Since the account was no longer being used
- ◉ While it's possible that lax password requirements and incorrect privileges may have contributed to the account compromise, the most glaring problem is that the terminated employee's account wasn't disabled. Since the account was no longer being used
- ○ While it's possible that strict password requirements and correct privileges may have contributed to the account compromise, the most glaring problem is that the terminated employee's account wasn't disabled. Since the account was no longer being used

7. For what type of account would interactive logon be disabled?

- Interactive logon refers to starting a OS. Service accounts do not require this type of access. Default superuser accounts, such as Administrator and root, may also be disabled, or limited to use in system recovery or repair.
- Interactive logon refers to starting a shell. Service accounts do not require this type of access. Default superuser accounts, such as Administrator and root, may also be enabled but limited to use in system recovery or repair.
- Interactive logon refers to starting a shell. Service accounts do not require this type of access. Default superuser accounts, such as Administrator and root, may also be disabled, or limited to use in system recovery or repair.
- Interactive logon refers to starting a OS. Service accounts do not require this type of access. Default superuser accounts, such as Administrator and root, may also be enabled but limited to use in system recovery or repair.

8. What container would you use if you want to apply a different security policy to a subset of objects within the same domain?

- Organization LAN (OL)
- Organization Unit (OU)
- Organization Bucket (OB)
- Organization Branch (OB)

9. Forcing users to change their password every month be counterproductive because more users would forget their password, try to select unsecure ones, or write them down/record them in a non-secure way (like a sticky note).

- True
- False

10. Enforce password history is the name of the policy that prevents users from choosing old passwords again?

- True
- False

11. Which is true about IP address, context-based authentication?

- An IP address cannot represent a logical location (subnet) on a private network. Most types of public IP address can be linked to a geographical location, based on information published by the registrant that manages that block of IP address space.
- An IP address can represent a logical location (subnet) on a private network. Most types of public IP address cannot be linked to a geographical location, based on information published by the registrant that manages that block of IP address space.
- An IP address can represent a logical location (subnet) on a private network. Most types of public IP address can be linked to a geographical location, based on information published by the registrant that manages that block of IP address space.
- An IP address cannot represent a logical location (subnet) on a private network. Most types of public IP address can be linked to a geographical location, based on information published by the registrant that manages that range of IP address space.

12. A user's actions are logged on the system. Each user is associated with a unique computer account. As long as the user's authentication is secure and the logging system is tamper-proof, they cannot deny having performed the action. Accounting does not provide non-repudiation.

- True
- False

13. Which information resource is required to complete usage auditing?

- Usage events must be recorded in a system record. Choosing which events to log will be guided by an audit policy.
- Usage events must be recorded in a spreadsheet. Choosing which events to log will be guided by an audit policy.
- Usage events must be recorded in a log. Choosing which events to log will be guided by an audit policy.
- Usage events must be recorded in a temp file. Choosing which events to log will be guided by an audit policy.

14. What is the difference between locked and disabled accounts?

- An account enters a locked state because of a policy violation, such as an incorrect password being entered incorrectly. Lockout is usually applied for a limited duration. An account is usually disabled manually, using the account properties. A disabled account can only be re-enabled manually.
- An account enters a blocked state because of a policy violation, such as an incorrect password being entered incorrectly. Lockout is usually applied for a limited duration. An

account is usually disabled manually, using the account properties. A disabled account can only be re-enabled manually.

- An account enters a locked state because of a policy violation, such as an the correct password being entered too many times. Lockout is usually applied for a limited duration. An account is usually disabled manually, using the account properties. A disabled account can only be re-enabled manually.
- An account enters a locked state because of a user issue, such as an incorrect password being entered incorrectly. Lockout is usually applied for a limited duration. An account is usually disabled manually, using the account properties. A disabled account can only be re-enabled manually.

15. What are the advantages of a decentralized, discretionary access control policy over a mandatory access control policy?

- It is easier for admins to adjust the policy to fit changing business needs. Centralized policies can easily become inflexible and bureaucratic.
- It is easier for users to adjust the policy to fit changing business needs. Centralized policies can easily become inflexible and bureaucratic.
- It is easier for users to adjust the policy to fit changing business needs. Decentralized policies can easily become inflexible and bureaucratic.
- It is easier for users to adjust the policy to fit changing business needs. Centralized policies are flexible and non-bureaucratic.

16. What is the difference between security group- and role-based permissions management?

- A container is simply a group of several user objects. Any organizing principle can be applied. In a role-based access control system, groups are tightly defined according to job functions. Also, a user should (logically) only possess the permissions of one role at a time.
- A group is simply a container for several user objects. Only a group-based organizing principle can be applied. In a role-based access control system, groups are tightly defined according to job functions. Also, a user should (logically) only possess the permissions of one role at a time.
- A group is simply a container for several user objects. Any organizing principle can be applied. In a role-based access control system, groups are tightly defined according to job functions. Also, a user should (physically) only possess the permissions of one role at a time.
- A group is simply a container for several user objects. Any organizing principle can be applied. In a role-based access control system, groups are tightly defined according to job functions. Also, a user should (logically) only possess the permissions of one role at a time.

17. In a rule-based access control model, can a subject negotiate with the data owner for access privileges? Why or why not?

- This sort of negotiation would not be permitted under rule-based access control; it is a feature of mandatory access control.
- This sort of negotiation would not be permitted under rule-based access control; it is a feature of discretionary access control.
- This sort of negotiation would be permitted under rule-based access control; it is not a feature of discretionary access control.
- This sort of negotiation would be permitted under rule-based access control; it is a feature of discretionary access control.

18. What is the purpose of directory services?

- To hide information about network resources and users in a format that can be accessed and updated using standard queries.
- To store information about network resources and users in a format that can be accessed and updated using standard queries.
- To store information about network devices in a format that can be accessed and updated using standard queries.
- To store information about network resources and users in a format that can never be accessed and updated using standard queries.

19. You are working on a cloud application that allows users to log on with social media accounts over the web and from a mobile application. Which protocols would you consider and which would you choose as most suitable?

- Security Association Markup Language (SAML) and Oauth + OpenID Connect (OIDC). OAuth with OIDC as an application layer offers better support for native mobile apps so is probably the best choice.
- Security Association Markup Language (SAML) and Oauth + OpenID Connect (OIDC). OAuth with OIDC as an authorization layer offers better support for native mobile apps so is probably the best choice.
- Security Association Markup Language (SAML) and Oauth + OpenID Connect (OIDC). OAuth with OIDC as an authentication layer offers better support for native mobile apps so is probably the best choice.
- Security Association Markup Language (SAML) and Oauth + OpenID Connect (OIDC). OAuth with OIDC as an data-link layer offers better support for native mobile apps so is probably the best choice.

20. A lack of proper user training directly contributes to the success of social engineering attempts. Attackers can easily trick users when those users are unfamiliar with the characteristics and ramifications of such deception.

- (●) True
- ( ) False

21. Why should an organization design role-based training programs?

- ( ) Employees typically have similar levels of technical knowledge and different work priorities. This means that a "one size fits all" approach to security training is practical.
- ( ) Employees have different levels of technical knowledge and different work ethics. This means that a "one size fits all" approach to security training is impractical.
- (●) Employees have different levels of technical knowledge and different work priorities. This means that a "one size fits all" approach to security training is impractical.
- ( ) Employees have different levels of technical knowledge and different work priorities. This means that a static approach to security training is practical.

22. You are planning a security awareness program for a manufacturer. Is a pamphlet likely to be sufficient in terms of resources?

- ( ) Using narrowly targeted training techniques will enforce engagement and retention. Practical tasks, such as phishing simulations, will give attendees more direct experience. Workshops or computer-based training will make it easier to assess whether the training has been completed.
- ( ) Using a diversity of training techniques will boost engagement and retention. physical tasks, such as phishing simulations, will give attendees more direct experience. Workshops or computer-based training will make it easier to assess whether the training has been completed.
- (●) Using a diversity of training techniques will boost engagement and retention. Practical tasks, such as phishing simulations, will give attendees more direct experience. Workshops or computer-based training will make it easier to assess whether the training has been completed.
- ( ) Using a diversity of training techniques will boost engagement and retention. Practical tasks, such as phishing simulations, will give attendees more direct experience. Workshops or computer-based training are largely considered to be ineffective.

2.2

1. In general, you should start implementing some form of network segmentation to put hosts with the same security requirements within segregated zones. For example, the workstations in each business department can be grouped in their own subnets to prevent a compromise of one subnet from spreading to another. Likewise, with VLANs, you can more easily manage the logical segmentation of the network without disrupting the physical infrastructure (i.e., devices and cabling).

- (●) True

- False

2. The Internet is an external zone where none of the hosts accessing your services can be assumed trusted or authenticated. An extranet is a zone allowing controlled access to semi-trusted hosts, implying some sort of authentication. The hosts are semi-trusted because they are not under the administrative control of the organization (as they are owned by suppliers, customers, business partners, contractors, and so on).

- True
- False

3. Why is subnetting useful in secure network design?

- Subnet traffic is not routed, therefore allowing pass through filtering devices such as a firewall.
- Subnet traffic is outward bound only. There is no need to secure it internally.
- Subnet traffic is routed, allowing it to be filtered by devices such as a firewall.
- Subnet traffic is local only preventing any leaking of packets to the external networks.

4. How can an enterprise DMZ be implemented?

- By using two firewalls around a screened subnet, or by using a triple-homed firewall
- By using three firewalls around a screened subnet, or by using a dual-homed firewall
- By using three firewalls around a screened subnet, or by using a triple-homed firewall
- By using two firewalls around a screened subnet, or by using a dual-homed firewall

5. What type of network requires the design to account for east-west traffic?

- This is an atypical design for a data center or server farm. Internal communications are considered to be "north-south".
- This is an atypical of a data center or server farm, where a single external request causes multiple cascading requests between servers within the data center.
- This is typical of a data center or server farm, where a single external request causes multiple cascading requests between servers within the data center.
- This is typical of a data center or server farm. It prevents a single external request from causing multiple cascading requests between servers within the data center creating congestion.

6. Why might an ARP poisoning tool be of use to a threat actor performing network reconnaissance?

- An ARP Poisoning Attack would never be used to perform reconnaissance. It is a DoS not used for Enumeration.
- The attacker can use ARP Poisoning to trick specifically targeted computers into sending traffic through the attacker's computer and, therefore, examine traffic that would not normally be accessible.
- An ARP Poisoning Attack could be used to perform reconnaissance. It is an atypical use of the tool but it would show details of dropped packets.
- The attacker could trick computers into sending traffic through the attacker's computer and, therefore, examine traffic that would not normally be accessible.

7. How could you prevent a malicious attacker from engineering a switching loop from a host connected to a standard switch port?

- Spanning Topology Protocol (STP) prevents switching loops.
- Enable the appropriate guards (portfast and BPDU Guard) on access ports.
- Use switch-based IP forwarding and filtering protocols like BPDU.
- Bridge buffers can be placed inline between the malicious attacker and the switch.

8. What port security feature mitigates ARP poisoning?

- Static ARP inspection—this does not relies upon DHCP snooping being enabled.
- Static ARP inspection—though this relies upon DHCP snooping being enabled.
- Dynamic ARP inspection—though this relies upon DHCP snooping being enabled.
- Dynamic ARP inspection—Note: DHCP snooping be disabled in the BIOS

9. What is a dissolvable agent?

- It is a Linux technology were the Daemon only lives in the computer's RAM and is deleted upon restart.
- It is an agent that is executed in the host's memory and CPU but not installed to a local disk.
- It is a Apple / Macintosh technology were the Daemon only lives in the computer's RAM and is deleted upon restart.
- It is a memory-based application used on phones and portable devices due to their limited storage capacity.

10. True or false? Band selection has a critical impact on all aspects of the security of a wireless network?

- ○ True
- ◉ False

11. The network manager is recommending the use of "thin" access points to implement the wireless network. What additional appliance or software is required and what security advantages should this have?

- ◉ You need a wireless controller to configure and manage the access points. This makes each access point more tamper-proof as there is no local administration interface. Configuration errors should also be easier to identify.
- ○ You do not need a wireless controller to configure and manage the access points. This makes each access point more tamper-proof as there is no local administration interface. Configuration errors should also be easier to identify.
- ○ You need a wireless controller to configure and manage the access points. This makes each access point more tamper-proof. There is a local administration interface, therefore, configuration errors should also be easier to identify.
- ○ You do not need a wireless controller to configure and manage the access points. This makes each access point more tamper-proof as there is no local administration interface. Configuration errors are difficult to identify because the node configuration cascades from the primary WAP controller.

12. What is a pre-shared key?

- ○ This is a type of group authentication used when the infrastructure for authenticating securely (via RADIUS, for instance) is additionally available. The system depends on the strength of the passphrase used for the key.
- ○ This is a type of group authentication used when the infrastructure for authenticating securely (via RADIUS, for instance) is not available. The system does not depend on the strength of the passphrase used for the key.
- ◉ This is a type of group authentication used when the infrastructure for authenticating securely (via RADIUS, for instance) is not available. The system depends on the strength of the passphrase used for the key.
- ○ This is a type of group authentication used when the infrastructure for authenticating securely (via KERBEROS, for instance) is not available. The system depends on the strength of the passphrase used for the key.

13. Is WPS a suitable authentication method for enterprise networks?

- No, an enterprise network will use RADIUS authentication. WPS uses PKI and there are weaknesses in the protocol.
- No, if the enterprise network uses TACAS+ authentication. WPS uses PSK and there are weaknesses in the protocol.
- No, an enterprise network will also need to use a tunneling protocol like VPNs for authentication. WPS uses PSK and there are weaknesses in the protocol.
- No, an enterprise network will use RADIUS authentication. WPS uses PSK and there are weaknesses in the protocol.

14. You want to deploy a wireless network where only clients with domainissued digital certificates can join the network. What type of authentication mechanism is suitable?

- LEAP-TLS is the best choice because it requires that both server and client be installed with valid certificates.
- AD is the best choice because it requires that both server and client be installed with valid certificates.
- LDAP is the best choice because it requires that both server and client be installed with valid certificates.
- EAP-TLS is the best choice because it requires that both server and client be installed with valid certificates.

15. John is given a laptop for official use and is on a business trip. When he arrives at his hotel, he turns on his laptop and finds a wireless access point with the name of the hotel, which he connects to for sending official communications. He may become a victim of which wireless threat?

- Crazy Uncle
- Evil Twin
- Redheaded Step Child
- Old Maid

16. Why are many network DoS attacks distributed?

- They are not often distributed attacks because those are easy to detect and mitigate.
- Most attacks depend on overwhelming the victim. This typically requires a large number of hosts, or bots.
- They are often distributed attacks because those are difficult to detect and mitigate.

- Most attacks depend on tricking the victim. This typically requires a large number of hosts, or bots in order to enumerate a system.

17. What is an amplification attack?

- Where the attacker sniffs the victim's IP in requests to several reflecting servers (often DNS or NTP servers). The attacker crafts the request so that the reflecting servers respond to the victim's IP with a large message, overwhelming the victim's bandwidth.
- Where the attacker spoofs the victim's IP in requests to several handler servers (often DNS or NTP servers). The attacker crafts the request so that the reflecting servers respond to the victim's IP with a large message, overwhelming the victim's bandwidth.
- Where the attacker spoofs the victim's IP in requests to several reflecting servers (often S/MIME or POP3 servers). The attacker crafts the request so that the reflecting servers respond to the victim's IP with a large message, overwhelming the victim's bandwidth.
- Where the attacker spoofs the victim's IP in requests to several reflecting servers (often DNS or NTP servers). The attacker crafts the request so that the reflecting servers respond to the victim's IP with a large message, overwhelming the victim's bandwidth.

18. What is meant by scheduling in the context of load balancing?

- The algorithm and metrics that determine which node a load balancer picks to handle a request.
- The algorithm and analytics that determine which node a load balancer picks to handle a request.
- The Pseudo Random Number Generator (PRNG) and metrics that determine which node a load balancer picks to handle a request.
- The algorithm and metrics that guarantee which node a load balancer picks to handle a request.

19. What mechanism provides the most reliable means of associating a client with a particular server node when using load balancing?

- Persistence is a layer 6 mechanism that works by injecting a session cookie. This is generally more reliable than the layer 2 source IP affinity mechanism.
- Persistence is a layer 7 mechanism that works by injecting a session cookie. This is generally more reliable than the layer 3 source IP affinity mechanism.
- Persistence is a layer 7 mechanism that works by injecting a session cookie. This is generally more reliable than the layer 4 source IP affinity mechanism.

- Persistence is a layer 6 mechanism that works by injecting a session cookie. This is generally more reliable than the layer 4 source IP affinity mechanism.

20. True or false? A virtual IP is a means by which two appliances can be put in a fault tolerant configuration to respond to requests for the same IP address?

- True.
- False

21. What field provides traffic marking for a QoS system at layer 3?

- Layer 3 refers to the DiffServ field in the IP header.
- False

2.3

1. True or False? As they protect data at the highest layer of the protocol stack, application-based firewalls have no basic packet filtering functionality.

- True. Only certain firewall types can perform basic packet filtering (by IP address, protocol type, port number, and so on).
- False. All firewall types can perform basic packet filtering (by IP address, protocol type, port number, and so on).

2. What distinguishes host-based personal software firewall from a network firewall appliance?

- A personal firewall software can block processes from accessing a network connection as well as applying filtering rules. A personal firewall protects the local host only, while a network firewall filters all traffic.
- A network firewall software can block processes from accessing a network connection as well as applying filtering rules. A network firewall protects the local host only, while a personal firewall filters traffic for all hosts on the segment behind the firewall.
- A personal firewall software can block processes from accessing a network connection as well as applying filtering rules. A personal firewall protects the local host only, while a network firewall filters traffic for all hosts on the segment behind the firewall.
- A personal firewall software can block processes from accessing a network connection as well as applying filtering rules. A network firewall protects the local host only, while a network firewall filters traffic for all hosts on the segment behind the firewall.

3. True or false? When deploying a non-transparent proxy, you must configure clients with the proxy address and port.

- (●) True.
- ( ) False.

4. What is usually the purpose of the default rule on a firewall?

- ( ) Allow all traffic not specifically allowed (implicit allow).
- (●) Block any traffic not specifically allowed (implicit deny).
- ( ) Block all unspecified traffic (implicit deny).
- ( ) Allow any unspecified traffic (implicit allow).

5. True or false? Static NAT means mapping a single public/external IP address to a single private/internal IP address.

- (●) True.
- ( ) False.

6. What is the best option for monitoring traffic passing from host-to-host on the same switch?

- ( ) The preferred option for monitoring intra-switch traffic is to use a mirrored port.
- ( ) The only option for monitoring intra-switch traffic is to use an ethernet cable tap.
- ( ) The preferred option for monitoring intra-switch traffic is to use an ethernet cable tap.
- (●) The only option for monitoring intra-switch traffic is to use a mirrored port.

7. What sort of maintenance must be performed on signature-based monitoring software?

- (●) Installing definition/signature updates and removing definitions that are not relevant to the hosts or services running on your network.
- ( ) Removing definitions that are not relevant to the hosts or services running on your network.
- ( ) Installing definition/signature updates.
- ( ) Installing definition/antivirus updates and removing definitions that are not relevant to the hosts or services running on your network.

8. What is the principal risk of deploying an intrusion prevention system with behavior-based detection?

- Behavior-based detection will exhibit high false positive rates, where legitimate activity is wrongly identified as malicious. With automatic prevention, this will block many legitimate users and hosts from the network, causing availability and support issues.
- Behavior-based detection can exhibit high false positive rates, where legitimate activity is wrongly identified as malicious. With automatic prevention, this will block many legitimate users and hosts from the network, causing availability and support issues.
- Behavior-based detection always exhibit high false positive rates, where legitimate activity is wrongly identified as malicious. With automatic prevention, this will block many legitimate users and hosts from the network, causing availability and support issues.
- Behavior-based detection never exhibits high false positive rates, where legitimate activity is wrongly identified as malicious. With automatic prevention, this will block many legitimate users and hosts from the network, causing availability and support issues.

9. If a Windows system file fails a file integrity check, should you suspect a malware infection?

- Yes—malware is a likely cause that you should investigate.
- No—malware is an unlikely cause.

10. What is a WAF?

- A web application firewall (WAF) is designed to protect HTTP and HTTPS applications. It can be configured with signatures of known attacks against applications, such as injection-based attacks or scanning attacks.
- A web application firewall (WAF) is designed to protect FTP and HTTPS applications. It can be configured with signatures of known attacks against applications, such as injection-based attacks or scanning attacks.
- A web application firewall (WAF) is designed to protect HTTP and HTTPS applications. It can be configured with fingerprints of known attacks against applications, such as injection-based attacks or scanning attacks.
- A web application firewall (WAF) is designed to protect HTTP and HTTPS applications. It can be configured with signatures of known attacks against applications, such as cross-site scripting attacks or scanning attacks.

11. What is the purpose of SIEM?

- Security information and event management (SIEM) products disseminates IDS alerts and host logs from multiple sources, then perform correlation analysis on the observables collected to identify indicators of compromise and alert administrators to potential incidents.
- Security information and event management (SIEM) products upload IDS alerts and host logs from multiple sources, then perform correlation analysis on the observables collected to identify indicators of compromise and alert administrators to potential incidents.
- Security information and event management (SIEM) products aggregate IDS alerts and host logs from multiple sources, then perform correlation analysis on the observables collected to identify indicators of compromise and alert administrators to potential incidents.
- Security information and event management (SIEM) products download IDS alerts and host logs from multiple sources, then perform correlation analysis on the observables collected to identify indicators of compromise and alert administrators to potential incidents.

12. What is the difference between a sensor and a collector, in the context of SIEM?

- A SIEM collector stores inputs (such as log files or packet traces) in a standard format that can be recorded within the SIEM and interpreted for event correlation. A sensor collects data from network devices.
- A SIEM collector transmits inputs (such as log files or packet traces) using a standard format that can be recorded within the SIEM and interpreted for event correlation. A sensor collects data from the servers.
- A SIEM collector parses inputs (such as log files or packet traces) into a standard format that can be recorded within the SIEM and interpreted for event correlation. A sensor collects data from the network media.
- A SIEM collector stores outputs (such as log files or packet traces) into a standard format that can be recorded within the SIEM and interpreted for event correlation. A sensor collects data from the network media.

13. Does Syslog perform all the functions of a SIEM?

- Yes, syslog is the embedded SIEM in Windows Server 2008 and all later versions.
- No, syslog allows remote hosts to send logs to a server, but syslog does not aggregate/ normalize the log data or run correlation rules to identify alertable events.

14. You are writing a shell script to display the last 5 lines of a log file at /var/ log/audit in a dashboard. What is the Linux command to do this?

- tail /var/log/audit -n 10
- head /var/log/audit -n 10

- tail /var/log/audit -n 5
- head /var/log/audit -n 5

15. What is the principal use of grep in relation to log files?

- grep is used to search the content of log files.
- grep is used to search the contents of shared directories.
- grep is used to search the contents of a compressed file.
- grep is used to search the content of the active mounted drive.

2.4

1. Denial of service (providing an invalid address configuration) and spoofing (providing a malicious address configuration—one that points to a malicious DNS, for instance) are vulnerabilities that a rogue DHCP server can expose users to?

- True
- False

2. DNS resolves domain names. If it were to be corrupted, users could be directed to spoofed websites. Disrupting DNS can also perform denial of service.

- True
- False

3. The contents of the HOSTS file are irrelevant as long as a DNS service is properly configured.

- True
- False

4. DNS server cache poisoning works by corrupting the records of a DNS server to point traffic destined for a legitimate domain to a malicious IP address.

- True
- False

5. DNSSEC depends on a chain of trust from the root servers down.

- (•) True
- ( ) False

6. What are the advantages of SASL over LDAPS?

- ( ) The Simple Authentication and Security Layer (SASL) forces the network administrator to choose SSL as the default authentication for signing and encryption (sealing)/integrity (signing) mechanism. By contrast, LDAPS uses Transport Layer Security (TLS) to encrypt traffic, but users still authenticate via simple binding. Also, SASL is the standards-based means of configuring LDAP security.
- ( ) The Simple Authentication and Security Layer (SASL) forces the network administrator to choose SSL as the default authentication for signing and encryption (sealing)/integrity (signing) mechanism. By contrast, LDAPS choose from a variety of technologies and vendors to encrypt traffic, but users still authenticate via simple binding. Also, SASL is the standards-based means of configuring LDAP security.
- (•) The Simple Authentication and Security Layer (SASL) allows a choice of authentication providers and encryption (sealing)/integrity (signing) mechanisms. By contrast, LDAPS uses Transport Layer Security (TLS) to encrypt traffic, but users still authenticate via simple binding. Also, SASL is the standards-based means of configuring LDAP security.
- ( ) The Simple Authentication and Security Layer (SASL) allows a choice of authentication providers and encryption (sealing)/integrity (signing) mechanisms. By contrast, LDAPS uses Transport Layer Security (TLS) to encrypt traffic, but users still authenticate via simple binding. Also, SASL is the defacto-based means of configuring LDAP security.

7. What steps should you take to secure an SNMPv2 service?

- ( ) Configure strong community names and use MOUs to restrict management operations to known hosts.
- ( ) Configure strong community names and use PBXs to restrict management operations to known hosts.
- (•) Configure strong community names and use ACLs to restrict management operations to known hosts.
- ( ) Configure strong community names and use RSAs to restrict management operations to known hosts.

8. What type of attack against HTTPS aims to force the server to negotiate weak ciphers?

- A downgrade attack.
- An upgrade attack.
- A single-sideband attack
- An out-of-band attack

9. A client and server have agreed on the use of the cipher suite ECDHE-ECDSAAES256- GCM-SHA384 for a TLS session. What is the key strength of the symmetric encryption algorithm?

- 256-bit (AES).
- 256-bit (RSA).
- 256-bit (SHA).
- 256-bit (MD5).

10. What security protocol does SFTP use to protect the connection and which port does an SFTP server listen on by default?

- SSH over UDP port 22.
- SSH over TCP port 22.
- TLS over TCP port 443.
- TLS over UDP port 443.

11. Which port(s) and security methods should be used by a mail client to submit messages for delivery by an SMTP server?

- Port 587 with STARTTLS (explicit TLS) or port 465 with implicit TLS.
- Port 465 with STARTTLS (explicit TLS) or port 587 with implicit TLS.
- Port 578 with STARTTLS (explicit TLS) or port 456 with implicit TLS.
- Port 456 with STARTTLS (explicit TLS) or port 578 with implicit TLS.

12. The recipient's public key (principally). The public key is used to encrypt a symmetric session key and (for performance reasons) the session key does the actual data encoding. The session key and, therefore, the message text can then only be recovered by the recipient, who uses the linked private key to decrypt it. In contrast, S/MIME uses the recipient's private key to encrypt a message.

- True

- (●) False

13. Which protocol protects the contents of a VoIP conversation from eavesdropping?

- ( ) STP
- ( ) ESP
- (●) SRTP
- ( ) SSTP

14. A TLS VPN can only provide access to web-based network resources.

- ( ) True
- (●) False - Transport Layer Security (TLS) VPN uses TLS to encapsulate the privatenetwork data and tunnel it over the network. The private network data could be frames or IP-level packets and is not constrained by application-layer protocol type.

15. What is Microsoft's TLS VPN solution?

- ( ) STP
- (●) SSTP
- ( ) ESP
- ( ) SRTP

16. What IPSec mode would you use for data confidentiality on a private network?

- ( ) STP
- ( ) SRTP
- (●) ESP
- ( ) SSTP

17. Which protocol is often used in conjunction with IPSec to provide a remote access client VPN with user authentication?

- (●) L2TP

- L3TP
- L2PT
- L3PT

18. What is the main advantage of IKE v2 over IKE v1?

- IKEv2 is faster and has less protocol overhead.
- IKEv2 is more secure because it uses EAP.
- IKEv2 is more secure because it uses LEAP.
- IKEv2 is faster because it uses SHA1024.

19. The server's public key (host key) confirms the identity of an SSH server to a client. Note that this can only be trusted if the client trusts that the public key is valid. The client might confirm this manually or using a Certificate Authority.

- True
- False

2.5

1. What use is made of a TPM for NAC attestation?

- The Trusted Platform Module (TPM) is a tamper-proof (at least in theory) cryptographic module embedded in the CPU or chipset. This can provide a means to sign the report of the system configuration so that a Active Directory (AD) policy enforcer can trust it.
- The Trusted Platform Module (TPM) is not tamper-proof. It is a cryptographic module embedded in the CPU or chipset. This can provide a means to sign the report of the system configuration so that a network access control (NAC) policy enforcer can trust it.
- The Trusted Platform Module (TPM) is a tamper-proof (at least in theory) cryptographic module inserted in USB port. This can provide a means to sign the report of the system configuration so that a network access control (NAC) policy enforcer can trust it.
- The Trusted Platform Module (TPM) is a tamper-proof (at least in theory) cryptographic module embedded in the CPU or chipset. This can provide a means to sign the report of the system configuration so that a network access control (NAC) policy enforcer can trust it.

2. Why are OS-enforced file access controls not sufficient in the event of the loss or theft of a computer or mobile device?

- The disk (or other storage) could be attached to a foreign system and the administrator could fake ownership of the files. File-level, full disk encryption (FDE), or self-encrypting drives (SED) mitigate this by requiring the presence of the user's decryption key to read the data.
- The disk (or other storage) could be attached to a foreign system and the administrator could take ownership of the files. File-level, full disk encryption (FDE), or self-encrypting drives (SED) mitigate this by requiring the presence of the user's decryption key to read the data.
- The disk (or other storage) could be attached to a foreign system and the administrator could take ownership of the files. File-level, full disk encryption (FDE), or self-encrypting drives (SED) help mitigate this by requiring the presence of the user's decryption key to change ownership of the data.
- The disk (or other storage) could be attached to a network file system (NFS) and a network administrator could take ownership of the files. File-level, full disk encryption (FDE), or self-encrypting drives (SED) mitigate this by requiring the presence of the user's decryption key to read the data.

3. What use is a TPM when implementing full disk encryption?

- A trusted platform module provides a secure mechanism for creating and storing the key used to encrypt the data. Access to the key is provided by configuring a password. The alternative is usually to store the private key on a USB stick.
- A trusted platform module provides a secure mechanism for creating and storing the key used to encrypt the data. Access to the key is provided by configuring a password. The alternative is usually to store the public key on a USB stick.
- A trusted platform module provides a semi-secure mechanism for creating and storing the key used to encrypt the data. Access to the key is provided by configuring a password. The alternative is usually to store the private key on a USB stick.
- A trusted platform module provides a semi-secure mechanism for creating and storing the key used to encrypt the data. Access to the key is provided by username and password. The alternative is usually to store the private key on a RFID media.

4. What countermeasures can you use against the threat of malicious firmware code?

- Only use reputable suppliers for peripheral devices and strictly controlled sources for firmware updates. Consider use of a chip dip sandboxed system to observe a device before allowing it to be attached to a host in the enterprise network. Use execution control software to allow only approved USB vendors.
- Only use reputable suppliers for peripheral devices and strictly controlled sources for firmware updates. Consider use of a wolf dip sandboxed system to observe a device before allowing it to be attached to a host in the enterprise network. Use execution control software to allow only approved USB vendors.
- Only use reputable suppliers for peripheral devices and strictly controlled sources for firmware updates. Consider use of a shark dip sandboxed system to observe a device before

allowing it to be attached to a host in the enterprise network. Use execution control software to allow only approved USB vendors.

- Only use reputable suppliers for peripheral devices and strictly controlled sources for firmware updates. Consider use of a sheep dip sandboxed system to observe a device before allowing it to be attached to a host in the enterprise network. Use execution control software to allow only approved USB vendors.

5. What type of interoperability agreement would be appropriate at the outset of two companies agreeing to work with one another?

- Non-Disclosure Agreement (NDA)
- Business Partnership Agreement (BPA)
- A memorandum of understanding (MOU).
- Service Level Agreement (SLA)
- Measurement Systems Analysis (MSA)

6. What type of interoperability agreement is designed to ensure specific performance standards?

- SLA and NDA
- SLA and BPA
- MSA and BPA
- MOU and BPA
- MOU and BPA

7. Only Microsoft's operating systems and applications require security patches.

- True - Only Microsoft products require security patches.
- False - Any vendor's or open source software or firmware can contain vulnerabilitiesthat need patching.

8. What is a hardened configuration?

- A basic principle of security is to run any services that are needed. A hardened system is configured to perform a role as client or application server with the minimal possible attack surface, in terms of interfaces, ports, services, storage, system/registry permissions, lack of security controls, and vulnerabilities.

- A basic principle of security is to run only services that are needed. A hardened system is configured to perform a role as client and/or application server with the minimal possible attack surface, in terms of interfaces, ports, services, storage, system/registry permissions, lack of security controls, and vulnerabilities.
- A basic principle of security is to run only services that are needed. A hardened system is configured to perform a role as client or application server with the minimal possible attack surface, in terms of interfaces, ports, services, storage, system/registry permissions, lack of security controls, and vulnerabilities.
- A basic principle of security is to run only services that are wanted. A hardened system is configured to perform a role as client or application server with the minimal possible attack surface, in terms of interfaces, ports, services, storage, system/registry permissions, lack of security controls, and vulnerabilities.

9. Anti-virus software has reported the presence of malware but cannot remove it automatically. Apart from the location of the affected file, what information will you need to remediate the system manually?

- The variable identifying the malware. You can use this to reference the malware on the A-V vendor's site and, hopefully, obtain manual removal and prevention advice.
- The string identifying the malware. You can use this to reference the malware on the A-V vendor's site and, hopefully, obtain manual removal and prevention advice.
- The integer identifying the malware. You can use this to reference the malware on the A-V vendor's site and, hopefully, obtain manual removal and prevention advice.
- The input identifying the malware. You can use this to reference the malware on the A-V vendor's site and, hopefully, obtain manual removal and prevention advice.

10. You are consulting with a medium-size company about endpoint security solutions. What advantages does a cloud-based analytics platform have over an on-premises solution that relies on signature updates?

- Advanced persistent threat (APT) malware can use many techniques to evade signature-based detection. A cloud analytics platform, backed by machine learning, can apply more effective behavioral-based monitoring and alerting.
- Advanced persistent threat (APT) malware can use many techniques to evade heuristic detection. A cloud analytics platform, backed by machine learning, can apply more effective behavioral-based monitoring and alerting.
- Advanced persistent threat (APT) malware can use many techniques to evade signature-based detection. A cloud analytics platform, backed by machine learning, are not yet an effective behavioral-based monitoring and alerting system.
- Advanced persistent threat (APT) malware can use many techniques to evade heuristic detection. A cloud analytics platform, backed by machine learning, are not yet an effective behavioral-based monitoring and alerting system.

11. If you suspect a process of being used for data exfiltration but the process is not identified as malware by A-V software, what types of analysis tools will be most useful?

- You can use a SLA with monitoring tools to see which files the process interacts with and a network monitor to see if it opens (or tries to open) a connection with a remote host.
- You can use a sandbox with monitoring tools to see which files the process interacts with and a network monitor to see if it opens (or tries to open) a connection with a remote host.
- You can use a TPM with monitoring tools to see which files the process interacts with and a network monitor to see if it opens (or tries to open) a connection with a remote host.
- You can use an escrow network with monitoring tools to see which files the process interacts with and a network monitor to see if it opens (or tries to open) a connection with a remote host.

12. Which of the following answers refers to a hierarchical system for the creation, management, storage, distribution, and revocation of digital certificates?

- Web of Trust
- PKI
- IaaS
- CA

13. A type of trusted third party that issues digital certificates used for creating digital signatures and public-private key pairs is known as:

- IKE
- CA
- PKI
- CSP

14. Which of the following certificate formats is used to store a binary representation of a digital certificate?

- PFX
- DER
- P7B
- PEM

15. A digital certificate which allows multiple domains to be protected by a single certificate is known as:

- ○ Extended Validation (EV) Certificate
- ○ Wildcard Certificate
- ◉ Subject Alternative Name (SAN) Certificate
- ○ Root Signing Certificate

16. Which digital certificate type allows multiple subdomains to be protected by a single certificate?

- ○ Root signing certificate
- ○ Subject Alternative Name (SAN) certificate
- ○ Extended Validation (EV) certificate
- ◉ Wildcard certificate

17. The term "Certificate chaining" refers to a process of verifying the authenticity of a newly received digital certificate. Such process involves checking all of the certificates in the chain of certificates from a trusted root CA, through any intermediate CAs, down to the certificate issued to the end user. A new certificate can only be trusted if each certificate in that certificate's chain is properly issued and valid.

- ◉ True
- ○ False

18. Copies of lost private encryption keys can be retrieved from a key escrow by recovery agents. Recovery agent is an individual with access to key database and permission level allowing him/her to extract keys from escrow.

- ◉ True
- ○ False

19. A trusted third-party storage solution providing backup source for cryptographic keys is referred to as:

- ◉ Key Escrow
- ○ TPM
- ○ Recovery Agent

- CA

20. Which of the answers listed below refer to examples of PKI trust models?

- Single CA model
- Hierarchical model (root CA + intermediate CAs)
- Mesh model (cross-certifying CAs)
- Web of trust model (all CAs act as root CAs)
- Client-server mutual authentication model
- All of the above

21. A security mechanism that allows HTTPS websites to resist impersonation by attackers using fraudulent certificates is called:

- Unified Threat Management (UTM)
- HTTP Public Key Pinning (HPKP)
- Data Execution Prevention (DEP)
- Web Application Firewall (WAF)

22. Which of the following allows for checking digital certificate revocation status without contacting Certificate Authority (CA)?

- A. OCSP stapling
- Certificate Revocation List (CRL)
- Sideloading
- Certificate Signing Request (CSR)

23. Which of the answers listed below refers to a method for requesting a digital certificate?

- CBC
- CSR
- CFB
- CRL

24. What is the fastest way for validating a digital certificate?

- CRL
- Key Escrow
- OCSP
- CSR

25. Which of the following solutions allow to check whether a digital certificate has been revoked?

- CIRT
- CRL
- CSR
- Key Escrow

26. Which digital certificate formats are commonly used to store private keys?

- P7B
- PFX
- CER
- B12

27. Which of the answers listed below refers to the most common format in which Certificate Authorities (CA) issue certificates?

- CER
- PEM
- DER
- P7B

3.1

1. . Other than cost, which factor primarily constrains embedded systems in terms of compute and networking?

- Weight
- Ease of Programming
- Power
- Processing Speed

2. While fully customizable by the customer, embedded systems are based on either the Raspberry Pi or the Arduino design.

- True
- False

3. What addressing component must be installed or configured for NB-IoT?

- system identity module (SIM)
- subscriber identity module (SIM)
- subscriber identity microchip (SIM)
- subscriber integrated module (SIM)

4. Why should detailed vendor and product assessments be required before allowing the use of IoT devices in the enterprise?

- As systems with considerable computing and networking functionality, these devices are subject to the same sort of vulnerabilities and exploits as ordinary workstations and laptops.
- As systems with limited computing and networking functionality, these devices are subject to the same sort of vulnerabilities and exploits as ordinary workstations and laptops.
- As systems with limited computing and networking functionality, these devices are not subject to the same sort of vulnerabilities and exploits as ordinary workstations and laptops.
- As systems with considerable computing and networking functionality, these devices are not subject to the same sort of vulnerabilities and exploits as ordinary workstations and laptops.

5. What type of deployment model(s) allow users to select the mobile device make and model?

- COPE & COBO
- BYOD & COBO
- COPE & CYOD

- BYOD & CYOD

6. How does VDI work as a mobile deployment model?

- Virtual Deployment Infrastructure (VDI) allows a client device to access a VM. In this scenario, the mobile device is the client device. Corporate data is stored and processed on the VM so there is less chance of it being compromised, even though the client device itself is not fully managed.
- Virtual Desktop Infrastructure (VDI) allows a client device to access a VM. In this scenario, the mobile device is the client device. Corporate data is stored and processed on the VM so there is less chance of it being compromised, even though the client device itself is not fully managed.
- Virtual Desktop Interface (VDI) allows a client device to access a VM. In this scenario, the mobile device is the client device. Corporate data is stored and processed on the VM so there is less chance of it being compromised, even though the client device itself is not fully managed.
- Virtual Deployment Interface (VDI) allows a client device to access a VM. In this scenario, the mobile device is the client device. Corporate data is stored and processed on the VM so there is less chance of it being compromised, even though the client device itself is not fully managed.

7. Company policy requires that you ensure your smartphone is secured from unauthorized access in case it is lost or stolen. To prevent someone from accessing data on the device immediately after it has been turned on, what security control should be used?

- Pattern Lock
- BIOS Password
- Screen lock
- TPM

8. An employee's car was recently broken into, and the thief stole a company tablet that held a great deal of sensitive data. You've already taken the precaution of securing plenty of backups of that data. What should you do to be absolutely certain that the data doesn't fall into the wrong hands?

- Initiate the table's self-destruct sequence.
- Use Find My Phone or similar app to locate the tablet.
- Remotely wipe the device, also referred to as a kill switch.
- It is a criminal issue. Do not interfere with the Police investigation.

9. A mobile app or workspace that runs within a partitioned environment to prevent other (unauthorized) apps from interacting with it is called containerization.

- (●) True
- ( ) False

10. Sideloading is when the user installs an app directly onto the device rather than from an official app store.

- (●) True
- ( ) False

11. Why might a company invest in device control software that prevents the use of recording devices within company premises?

- ( ) To not inadvertently violate any intellectual property rights.
- (●) To hinder physical reconnaissance and espionage.
- ( ) Such control software does not exist.
- ( ) Because a SOP or employee policy is not enough to keep people from bringing their phones to work.

12. A rooted or jailbroken devices are not a significant threat to enterprise security. Enterprise Mobility Management (EMM) solutions depend on the device user not being able to override their settings or change the effect of the software. A rooted or jailbroken device means that the user could subvert the access controls.

- ( ) True
- (●) False

13. An attacker can set up some sort of rogue access point (Wi-Fi) or cell tower (cellular) to perform eavesdropping or man-in-the-middle attacks. For Personal Area Network (PAN) range communications, there might be an opportunity for an attacker to run exploit code over the channel.

- (●) True
- ( ) False

14. Why might enforcement policies be used to prevent USB tethering when a smartphone is brought to the workplace?

- An enforcement policy would not allow a PC or laptop to connect to the Internet via the smartphone's cellular data connection by disabling the USB computer's ports.
- An enforcement policy would allow a PC or laptop to connect to the Internet via the computer's data connection. This could be used to evade network security mechanisms, such as data loss prevention or content filtering.
- This would allow a PC or laptop to connect to the Internet via the smartphone's cellular data connection. However, this could not be used to evade network security mechanisms, such as data loss prevention or content filtering.
- This would allow a PC or laptop to connect to the Internet via the smartphone's cellular data connection. This could be used to evade network security mechanisms, such as data loss prevention or content filtering.

15. A maliciously designed USB battery charger could be used to exploit a mobile device on connection.

- True
- False

16. Chuck, a sales executive, is attending meetings at a professional conference that is also being attended by representatives of other companies in his field. At the conference, he uses his smartphone with a Bluetooth headset to stay in touch with clients. A few days after the conference, he finds that competitors' sales representatives are getting in touch with his key contacts and influencing them by revealing what he thought was private information from his email and calendar. Chuck is a victim of which wireless threat?

- Bluemooning
- Bluesnarfing
- Bluesniffing
- Bluetuning

3.2

1. Your log shows that the Notepad process on a workstation running as the local administrator account has started an unknown process on an application server running as the SYSTEM account. What type of attack(s) are represented in this intrusion event?

- The Notepad process has been compromised, using integer overflow or a DLL/ process injection attack. The threat actor has then performed lateral movement and privilege escalation, gaining higher privileges through remote code execution on the application server.

- The Notepad process has been compromised, possibly using buffer overflow or a DLL/ process injection attack. The threat actor has then performed lateral movement and privilege escalation, gaining higher privileges through remote code execution on the application server.
- The Notepad process has been compromised, possibly using buffer overflow or a DLL/ sub-injection attack. The threat actor has then performed lateral movement and privilege escalation, gaining higher privileges through remote code execution on the application server.
- The Notepad process has been compromised, possibly using buffer overflow or a DLL/ process injection attack. The threat actor has not yet performed lateral movement and privilege escalation, gaining higher privileges through remote code execution on the application server.

2. How might an integer overflow be used as part of a buffer overflow?

- The integer value could be used to allocate less memory than a process expects, making a buffer overflow easier to achieve.
- The integer value could be used to allocate more memory than a process expects, making a buffer overflow impossible to achieve.
- The integer value could be used to allocate more memory than a process expects, making a buffer overflow harder to achieve.
- The integer value could be used to allocate more memory than a process expects, making a buffer overflow harder to achieve.

3. Real-time detection of a buffer overflow is difficult, and is typically only achieved by security monitoring software (antivirus, endpoint detection and response, or user and entity behavior analytics) or by observing the host closely within a sandbox. An unsuccessful attempt is likely to cause the process to crash with an error message. If the attempt is successful, the process is likely to show anomalous behavior, such as starting another process, opening network connections, or writing to AutoRun keys in the registry. These indicators can be recorded using logging and system monitoring tools.

- True
- False

4. What is the effect of a memory leak?

- A process claims memory locations but always releases them, reducing the amount of memory available to other processes. This will damage performance, could prevent other processes from starting, and if left unchecked could crash the OS.
- A process claims memory locations but never releases them, reducing the amount of memory available to other processes. This will damage performance, could prevent other processes from starting, and if left unchecked could crash the OS.

- A process claims memory locations but always releases them, reducing the amount of memory available to other processes. This will damage performance, could prevent other processes from starting, and if left unchecked could crash the OS.
- A process claims memory locations but never releases them, reducing the amount of memory available to other processes. This will not damage performance, but could prevent other processes from starting, and if left unchecked could crash the OS.

5. Various OS system functions allow one process to manipulate another and force it to load a dynamic link library (DLL). This means that the malware code cannot migrate from one process to another, evading detection.

- True
- False

6. Regarding Pass-the-Hash attacks: These attacks are revealed by use of certain modes of NTLM authentication within the security (audit) log of the source and target hosts. These indicators can be prone to false positives, however, as many services use NTLM authentication legitimately.

- True
- False

7. You are reviewing access logs on a web server and notice repeated requests for URLs containing the strings %3C and %3E. Is this an event that should be investigated further, and why?

- Those strings represent percent encoding for HTML tag delimiters (< and >). This could be an XML attempt to inject a script so should be investigated.
- Those strings represent percent encoding for HTML tag delimiters (< and >). This could be an XSS attempt to inject a script so should be investigated.
- Those strings represent decimal encoding for HTML tag delimiters (< and >). This could be an XLSX attempt to inject a script so should be investigated.
- Those strings represent decimal encoding for HTML tag delimiters (< and >). This could be an RSX attempt to inject a script so should be investigated.

8. You have been asked to monitor baseline API usage so that a rate limiter value can be set. What is the purpose of this?

- A rate limiter will not mitigate denial of service (DoS) attacks on the API, where a malicious entity generates millions of spurious requests to block legitimate ones. You need to establish a

baseline to ensure continued availability for legitimate users by setting the rate limit at an appropriate level.

- A rate limiter will not detect a denial of service (DoS) attacks on the API, where a malicious entity generates millions of spurious requests to block legitimate ones. You need to establish a baseline to ensure continued availability for legitimate users by setting the rate limit at an appropriate level.
- A rate limiter will mitigate denial of service (DoS) attacks on the API, where a malicious entity generates millions of spurious requests to block legitimate ones. You need to establish a baseline to ensure continued availability for legitimate users by setting the rate limit at an appropriate level.
- A rate limiter will detect denial of service (DoS) attacks on the API, where a malicious entity generates millions of spurious requests to block legitimate ones. You need to establish a baseline to ensure continued availability for legitimate users by setting the rate limit at an appropriate level.

9. How does a replay attack work in the context of session hijacking?

- The attacker captures some data, such as a cookie, used to log on or start a session legitimately. The attacker then encrypts the captured data to re-enable the connection.
- The attacker captures some data, such as a cookie, used to log on or start a session legitimately. The attacker then resends the captured data to disable the connection.
- The attacker captures some data, such as a cookie, used to log on or start a session legitimately. The attacker then resends the captured data to re-enable the connection.
- The attacker captures some data, such as a cookie, used to log on or start a session illegitimately. The attacker then resends the captured data to re-enable the connection.

10. How does a clickjacking attack work?

- The attacker inserts an invisible layer into a trusted web page that can intercept or redirect input without the user realizing.
- The attacker removes an invisible layer into a untrusted web page that can intercept or redirect input without the user realizing.
- The attacker removes an visible layer into a trusted web page that can intercept or redirect input without the user realizing.
- The attacker inserts an visible layer into a untrusted web page that can intercept or redirect input without the user realizing.

11. What is a persistent XSS attack?

- Where the attacker inserts a backdoor code into the back-end database used to serve content to the trusted site.
- Where the attacker inserts malicious code into the back-end spreadsheet used to serve content to the untrusted site.
- Where the attacker inserts malicious code into the back-end database used to serve content to the trusted site.
- Where the attacker inserts malicious code into the back-end spreadsheet used to serve content to the trusted site.

12. How might an attacker exploit a web application to perform a shell injection attack?

- The attacker does not need to find a vulnerable input method, such as a form control or URL or script parser, that will allow the execution of OS shell commands.
- The attacker does not need to find a vulnerable input method, such as a form control or URL or script parser, that will disallow the execution of OS shell commands.
- The attacker needs to find a vulnerable input method, such as a form control or URL or script parser, that will allow the execution of OS shell commands.
- The attacker needs to find a vulnerable input method, such as a form control or URL or script parser, that will disallow the execution of OS shell commands.

13. Server-side request forgery (SSRF) causes a public server to make an arbitrary request to a back-end server. This is made much harder if the threat actor has to defeat an authentication or authorization mechanism between the web server and the database server.

- True
- False

14. What type of programming practice defends against injection-style attacks, such as inserting SQL commands into a database application from a site search form?

- Input verification provides some mitigation against this type of input being passed to an application via a user form. Output encoding could provide another layer of protection by checking that the query that the script passes to the database is safe.
- Input validation provides some mitigation against this type of input being passed to an application via a user form. Output encoding could provide another layer of protection by checking that the query that the script passes to the database is safe.
- Input authentication provides some mitigation against this type of input being passed to an application via a user form. Output encoding could provide another layer of protection by checking that the query that the script passes to the database is safe.

- Input visualization provides some mitigation against this type of input being passed to an application via a user form. Output encoding could provide another layer of protection by checking that the query that the script passes to the database is safe.

15. Output encoding ensures that strings are made safe for the context they are being passed to, such as when a JavaScript variable provides output to render as HTML. Safe means that the string contains unauthorized syntax elements, such as script tags.

- True
- False

16. The document object model (DOM) is the means by which a script (JavaScript) can change the way a page is rendered. As this change is rendered by the browser, it is client-side code.

- True
- False

17. Which response header provides protection against SSL stripping attacks?

- HTTPS Strict Transport Security (HSTS).
- HTTPTLS Strict Transport Security (HSTS).
- HTTPSIP Strict Transport Security (HSTS).
- HTTP Strict Transport Security (HSTS).

18. A default error message will not reveal platform information and the workings of the code to an attacker.

- True
- False

19. A software development kit (SDK) contains tools and code examples released by a vendor to make developing applications within a particular environment (framework, programming language, OS, and so on) easier. No element in the SDK could contain vulnerabilities that could then be transferred to the developer's code or application.

- True
- False

20. A fuzzer can be used to submit known unsafe strings and randomized input to test whether they are made safe by input validation or not.

- True
- False

3.3

1. You have been asked to investigate a web server for possible intrusion. You identify a script with the following code. What language is the code in and does it seem likely to be malicious? import os, sockets, syslog def r_conn(ip) s=socket.socket(socket.AF_INET,socket.SOCK_DGRAM) s.connect(("logging.trusted.foo",514)) ...

- The code is written in Python. It uses various modules with default library code to interact with the OS and network, and also the syslog logging platform. The first lines of code define a function to connect to a host over port 514 (syslog). SOCK_DGRAM is a UDP connection, which is standard for syslog. Most likely the script is for remote logging and unlikely to be malicious, especially if trusted.foo is a known domain.
- The code is written in PHP. It uses various modules with default library code to interact with the OS and network, and also the syslog logging platform. The first lines of code define a function to connect to a host over port 514 (syslog). SOCK_DGRAM is a UDP connection, which is standard for syslog. Most likely the script is for remote logging and unlikely to be malicious, especially if trusted.foo is a known domain.
- The code is written in SQL. It uses various modules with default library code to interact with the OS and network, and also the syslog logging platform. The first lines of code define a function to connect to a host over port 514 (syslog). SOCK_DGRAM is a UDP connection, which is standard for syslog. Most likely the script is for remote logging and likely to be malicious, especially if trusted.foo is a known domain.
- The code is written in Ruby. It uses various modules with default library code to interact with the OS and network, and also the syslog logging platform. The first lines of code define a function to connect to a host over port 514 (syslog). SOCK_DGRAM is a UDP connection, which is standard for syslog. Most likely the script is for remote logging and likely to be malicious, especially if trusted.foo is a known domain.

2. You can restrict the use of PowerShell on Windows 10 clients. There are various group policy-based mechanisms, but for Windows 10, the Windows Defender Application Control (WDAC) framework provides the most powerful toolset for execution control policies.

- True
- False

3. A log shows that a PowerShell IEX process attempted to create a thread in the target image c:\Windows\System32\lsass.exe. What is the aim of this attack?

- The Local Security Authority Subsystem Service (LSASS) enforces security policies, including authentication and password changes. Consequently, it holds hashes of user passwords in memory. Attacks on lsass.exe are typically credential dumping to steal those hashes.
- The Local Security Authority Subsystem Service (LSASS) enforces security policies, including authentication and password changes. Consequently, it holds hashes of user passwords in memory. Attacks on lsass.exe are typically cryptomining.
- The Logical Security Authority Subsystem Service (LSASS) enforces security policies, including authentication and password changes. Consequently, it holds hashes of user passwords in memory. Attacks on lsass.exe are typically cryptomining.
- The Logical Security Authority Subsystem Service (LSASS) enforces security policies, including authentication and password changes. Consequently, it holds hashes of user passwords in memory. Attacks on lsass.exe are typically credential dumping to steal those hashes.

4. You are discussing a security awareness training program for an SME's employees. The business owner asserts that as they do not run Microsoft Office desktop apps, there should be no need to cover document security and risks from embedded macros and scripts. Should you agree and not run this part of the program?

- No. While Visual Basic for Applications (VBA) can only be used with Microsoft Office, other types of document can contain embedded scripts, such as JavaScript in PDFs. Other Office suites, such as OpenOffice and LibreOffice, use scripting languages for macros too.
- Yes. Visual Basic for Applications (VBA) can only be used with Microsoft Office, other types of document cannot contain embedded scripts, such as JavaScript in PDFs. Other Office suites, such as OpenOffice and LibreOffice, do not use scripting languages for macros.

5. Creating secure development environments for the different phases of a software development project (initial development server, test/integration server, staging [user test] server, production server). This is called secure setting or sandboxing.

- True
- False

6. What feature is essential for managing code iterations within the provisioning and deprovisioning processes?

- Version control is an ID system for each iteration of a software product.

- Version control is an code system for each large iteration of a software product.
- Variable control is an ID system for each iteration of a software product.
- Variable control is an code system for each iteration of a software product.

7. Which life cycle process manages continuous release of code to the production environment?

- Continuous deployment.
- Concentric deployment.
- Concentric development.
- Continuous development.

8. The compiler can apply obfuscation routines to make the code difficult for a threat actor to reverse engineer and analyze for vulnerabilities.

- True
- False

9. Which of the following answers refers to a TCP port used by FTP for session control?

- 20
- 22
- 21
- 25

10. An FTP data transfer connection is established through a TCP port number:

- 23
- 25
- 20
- 21

11. Which of the port number listed below is used by FTP over TLS/SSL (FTPS)?

- 20
- 989
- 5060
- 21
- 5061

12. Which of the following statements are true?

- Secure File Transfer Protocol (SFTP) runs by default on port 22
- Secure Copy (SCP) runs by default on port 22
- Secure Shell (SSH) runs by default on port 22
- All the above are true.

13. Dynamic Host Configuration Protocol (DHCP) runs on

- UDP port 63
- UDP port 64
- UDP port 65
- UDP port 66
- UDP port 67

14. Which port number is used by DNS?

- 53
- 67
- 110
- 389

15. HTTP is assigned to port 443

- True
- False

16. Which of the UDP port numbers listed below is assigned to the Internet Message Access Protocol (IMAP)?

- ○ 143
- ○ 389
- ○ 443
- ○ 636
- ◉ None of the above

17. IMAPS runs on SSL, TLS, and uses TCP port 993.

- ◉ True
- ○ False

18. Which protocol uses port 500?

- ○ L2TP
- ◉ IKE
- ○ POP3S
- ○ SIP
- ○ RSAKMP

19. Which of the following answers refers to a port number assigned to the Kerberos authentication system?

- ○ 49
- ◉ 88
- ○ 1645
- ○ 1723

20. Port 1701 is used by:

- ◉ L2TP

- RADIUS
- PPTP
- SMTPS

21. TCP port 389 is the default port for:

- RDP
- LDAP
- SMB
- RCP
- None of the above.

22. A network administrator has been asked to secure directory service access with an SSL/TLS encryption. Which of the following TCP ports needs to be opened to implement this change?

- 636
- 389
- 443
- 1701
- 1720

23. TCP port 119 is assigned to:

- IMAP
- POP3
- NTP
- NNTP
- None of the above.

24. Network Time Protocol (NTP) runs on TCP port:

- 123
- 110

- 161
- 137
- None of the above.

25. POP3 uses:

- UDP port 110
- UDP port 123
- TCP port 143
- TCP port 161
- None of the above.

26. POP3S uses SSL, TLS and UDP port 995.

- True
- False

27. Port 1701 is used by Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)

- True
- False

28. RADIUS uses which port:

- 989
- 5060
- 1812
- 990
- None of the above.

29. A network technician uses Remote Desktop Protocol (RDP) client on their Windows OS to remotely troubleshoot a problem on another Windows machine. Which of the following ports needs to be opened for the built-in Windows RDP server to allow this type of network connection?

- TCP port 389
- TCP port 636
- TCP port 3389
- TCP port 993

30. Unblocking port number 22 enables what type of traffic?

- SFTPS
- FTP
- TFTP
- SCP
- FTPS

31. SIP uses ports 5060 and 5061.

- True
- False

32. Port 25 is used by:

- SNMP
- Telnet
- FTP
- SMTP
- None of the above.

33. SMTPS uses SSL, TLS and TCP port 599.

- True
- False

34. An SNMP management station receives SNMP notifications from Agents on UDP port:

- 161
- 137
- 162
- 138

35. A network administrator has been asked to set up a VPN link on a connecting host with no dedicated VPN client application installed. Which of the following ports needs to be opened to enable this type of connection?

- 443
- 22
- 143
- 3389

36. Ports 514 and 6514 are used for syslog servers.

- True
- False

37. What is port 49 used for?

- TACACS+
- RADIUS
- KERBEROS
- LDAP

3.4

1. What is meant by a public cloud?

- A solution hosted by a third party cloud service provider (CSP) and shared between subscribers (multi-tenant). This sort of cloud solution has the greatest security concerns.

2. What type of cloud solution would be used to implement a SAN?

- This would usually be described as Infrastructure as a Service (IaaS).

3. What is a Type II hypervisor?

- Software that manages virtual machines that has been installed to a guest OS. This is in contrast to a Type I (or "bare metal") hypervisor, which interfaces directly with the host

4. What is a VDE?

- A Virtual Desktop Environment (VDE) is the workspace presented when accessing an instance in a virtual desktop infrastructure (VDI) solution. VDI is the whole solution (host server and virtualization platform, connection protocols, connection/session broker, and client access devices).

5. What is the risk from a VM escaping attack?

- VM escaping refers to attacking other guest OSes or the hypervisor or host from within a virtual machine. Attacks may be to steal information, perform Denial of Service (DoS), infect the system with malware, and so on.

6. Describe some key considerations that should be made when hosting data or systems via a cloud solutions provider.

- Integrate auditing and monitoring procedures and systems with on-premises detection, identify responsibility for implementing security controls (such as patching or backup), identify performance metrics in an SLA, and assess risks to privacy and confidentiality from breaches at the service provider.

7. True or false? The account with which you register for the CSP services is not an account with root privileges.

- False. This account is the root account and has full privileges. It should not be used for day-to-day administration or configuration.

8. Which security attribute is ensured by monitoring API latency and correcting any problems quickly?

- This ensures the availability of services.

9. What format is often used to write permissions statements for cloud resource policies?

- JavaScript Object Notation (JSON).

10. True or false? A customer is limited to creating one VPC per account.

- False. There are limits to the number of virtual private clouds (VPCs) that can be created, but more than one is allowed.

11. What feature allows you to filter traffic arriving at an instance?

- This is accomplished by assigning the instance to a security group with the relevant policy configured.

12. What is a cloud access security broker (CASB)?

- Enterprise management software mediating access to cloud services by users to enforce information and access policies and audit usage.

13. A company has been using a custom-developed client-server application for customer management, accessed from remote sites over a VPN. Rapid overseas growth has led to numerous complaints from employees that the system suffers many outages and cannot cope with the increased number of users and access by client devices such as smartphones. What type of architecture could produce a solution that is more scalable?

- Microservices is a suitable architecture for replacing monolithic client-server applications that do not meet the needs of geographically diverse, mobile workforces. By breaking the application up into microservice components and hosting these in cloud containers, performance can scale to demand. Web-based APIs are better suited to browser-based access on different device types.

14. You have been asked to produce a summary of pros and cons for the products Chef and Puppet. What type of virtualization or cloud computing technology do these support?

- These are orchestration tools. Orchestration facilitates "automation of automation," ensuring that scripts and API calls are made in the right order and at the right time to support an overall workflow.

15. True or false? Serverless means running computer code on embedded systems.

- False. With serverless, the provision of functions running in containers is abstracted from the underlying server hardware. The point is that as a consumer, you do not perform any server management. The servers are still present, but they are operated and maintained by the cloud service provider.

16. A company's web services are suffering performance issues because updates keep failing to run on certain systems. What type of architecture could address this issue?

- Infrastructure as Code (IaC) means that provisioning is performed entirely from standard scripts and configuration data. The absence of manual configuration adjustments or ad hoc scripts to change settings is designed to eliminate configuration drift so that updates run consistently between the development and production environments.

17. What is SDV?

- Software-defined visibility (SDV) gives API-based access to network infrastructure and hosts so that configuration and state data can be reported in near real time. This facilitates greater automation in models and technologies such as zero trust, inspection of east/west data center traffic, and use of security orchestration and automated response (SOAR) tools.