3.1 Benchmark

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 Benchmark

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 Benchmark

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.

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

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 TPC port 456.

- 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 Benchmark

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.

3.5 Benchmark

1. What is the difference between the role of data steward and the role of data custodian?

- The data steward role is concerned with the quantity of data (amount, labeling, nominalization, and so on). The data custodian role focuses on the system hosting the data assets and its access control mechanisms.
- The data steward role is concerned with the quantity of data (amount, labeling, nominalization, and so on). The data custodian role focuses on limiting outlying factors such as weather, earthquake, fire, flood and so on.
- The data steward role is concerned with the quality of data (format, labeling, normalization, and so on). The data custodian role focuses on the system hosting the data assets and its access control mechanisms.
- The data steward role is concerned with the quality of data (format, labeling, normalization, and so on). The data custodian role focuses on limiting outlying factors such as weather, earthquake, fire, flood and so on.

2. One set of information classifications tags could indicate the degree of confidentiality (public, confidential/secret, or critical/top secret). Another tagging schema could distinguish proprietary from private/sensitive personal data.

- True

3. PII is personally identifiable information is any data that could be used to identify, contact, or locate an individual.

- True

4. You are reviewing security and privacy issues relating to a membership database for a hobbyist site with a global audience. The site currently collects account details with no further information. What should be added to be in compliance with data protection regulations? True or False: The site should add a privacy notice explaining the purposes the personal information is collected and used for. The form should provide a means for the user to give explicit and informed consent to this privacy notice.

- True

5. You are preparing a briefing paper for customers on the organizational consequences of data and privacy breaches. You have completed sections for reputation damage, identity theft, and IP theft. Following the CompTIA Security+ objectives, what other section should you add?

- Data and privacy breaches can lead arbitrators or regulators to impose fines. In some cases, these fines can be substantial (calculated as a percentage of turnover).
- Data and privacy breaches can lead legislators or regulators to impose fines. In some cases, these fines can be substantial (calculated as a percentage of turnover).
- Data and privacy breaches can lead arbitrators or regulators to impose fines though these these fines can be inconsequential (calculated as a percentage of turnover).
- Data and privacy breaches can lead legislators or regulators to impose fines though these these fines can be inconsequential (calculated as a percentage of turnover).

6. To what data state does a trusted execution environment apply data protection?

- Data in use.
- Data in storage.

7. You take an incident report from a user trying to access a REPORT.docx file on a SharePoint site. The file has been replaced by a QUARANTINE.txt file containing a policy violation notice. What is the most likely cause?

- This is typical of a data loss prevention (DLP) policy replacing a file involved in a policy violation with a graveyard file.
- This is typical of a data loss prevention (DLP) policy replacing a file involved in a policy violation with a tombstone file.
- This is atypical of a data loss prevention (DLP) policy replacing a file involved in a policy violation with a graveyard file.
- This is atypical of a data loss prevention (DLP) policy replacing a file involved in a policy violation with a tombstone file.

8. You are preparing a solution overview on privacy enhancing technologies based on CompTIA Security+ syllabus objectives. You have completed notes under the following headings—which other report section do you need? Data minimization, Anonymization, Pseudo-anonymization, Data masking, Aggregation/Banding

- Tokenization—creating data with a randomly generated token from a separate token server or vault. This allows reconstruction of the original data if combined with the token vault.
- Tokenization—creating data with a pseudo-randomly generated token from a separate token server or vault. This allows reconstruction of the original data if combined with the token vault.
- Tokenization—replacing data with a pseudo-randomly generated token from a separate token server or vault. This allows reconstruction of the original data if combined with the token vault.
- Tokenization—replacing data with a randomly generated token from a separate token server or vault. This allows reconstruction of the original data if combined with the token vault.

9. Which of the answers listed below refers to a solution allowing administrators to block Internet access for users until they perform required action?

- Honeypot
- Quarantine network
- Captive portal
- Firewall

10. Wi-Fi Protected Setup (WPS) is a network security standard which simplifies configuration of new wireless networks by providing non-technical users with a capability to easily configure network security settings and add new devices to an existing network. WPS has known vulnerabilities and disabling this functionality is one of the recommended ways of securing wireless networks.

- True
- False

11. What are the characteristic features of WPA/WPA2 Enterprise mode?

- Suitable for small corporate networks
- Does not require an authentication server
- Suitable for all types of wireless LANs
- Requires RADIUS authentication server

12. Which of the following would be the best solution for securing a small network lacking an authentication server?

- WPA-PSK
- WPA2-Enterprise
- WPA2-PSK
- WPA-Enterprise

13. Extensible Authentication Protocol (EAP) is an authentication framework frequently used in wireless networks and point-to-point connections. EAP provides an authentication framework, not a specific authentication mechanism. There are many authentication mechanisms (referred to as EAP methods) that can be used with EAP. Wireless networks take advantage of several EAP methods, including PEAP, EAP-FAST, EAP-TLS, and EAP-TTLS.

- True
- False

14. Which of the EAP methods listed below relies on client-side and server-side certificates to perform authentication?

- EAP-TLS
- PEAP
- EAP-TTLS
- EAP-FAST

15. Which of the following EAP methods offers the highest level of security?

- PEAP
- EAP-FAST
- EAP-TLS
- EAP-TTLS

16. A security protocol designed to strengthen existing WEP implementations without requiring the replacement of legacy hardware is known as:

- PEAP
- TKIP
- CCMP
- WPA2

17. AES-based encryption mode implemented in WPA2 is known as:

- CCMP
- ECB
- CBC

- TKIP

18. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are encryption standards designed for securing wireless networks. WEP is an older standard and due to its vulnerabilities is not recommended. WPA was designed as an interim replacement for WEP, and WPA2 was introduced as the official standard offering the strongest security of the three.

- True
- False

19. A wireless disassociation attack is a type of:

- Downgrade attack
- Brute-force attack
- Denial of Service (Dos) attack
- Cryptographic attack

20. What is the name of a technology used for contactless payment transactions?

- NFC
- SDN
- PED
- WAP

21. Which of the following wireless technologies enables identification and tracking of tags attached to objects?

- WTLS
- GPS
- RFID
- WAF

22. Gaining unauthorized access to a Bluetooth device is referred to as:

- Phishing
- Bluejacking
- Tailgating
- Bluesnarfing

23. The practice of sending unsolicited messages over Bluetooth is called:

- SPIM
- Bluejacking
- Vishing

- Bluesnarfing

24. Which of the wireless technologies listed below are deprecated and should not be used due to their known vulnerabilities?

- WPS
- WAP
- WPA2
- WAF
- WEP

25. A wireless jamming attack is a type of:

- Cryptographic attack
- Denial of Service (Dos) attack
- Brute-force attack
- Downgrade attack

26. The term "Evil twin" refers to a rogue Wireless Access Point (WAP) set up for eavesdropping or stealing sensitive user data. Evil twin replaces the legitimate access point and by advertising its own presence with the same Service Set Identifier (SSID, a.k.a. network name) appears as a legitimate access point to connecting hosts.

- True
- False

27. A type of wireless attack designed to exploit vulnerabilities of WEP is known as:

- MITM attack
- Smurf attack
- IV attack
- Xmas attack

28. Which of the following security protocols is the least susceptible to wireless replay attacks?

- WPA2-CCMP
- WPA-TKIP
- WPA2-PSK
- WPA-CCMP
- WPA2-TKIP