CyberRookie CSX Fundamentals - Section 4: Security of Networks, Systems, Applications and Data

Quizlet

Study online at quizlet.com/_7r6gga

1. **4 main phases of penetration testing**	Planning, Discovery, Attack and Reporting
2. **802.11**	Refers to a family of specifications for wireless LAN technology.
3. **802.11**	Specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.
4. **8000**	HTTP- TCP/UDP
5. **8080**	HTTP- TCP/UDP
6. **31337**	Back Orifice - UDP
7. **the ability to network sniff**	Is becoming easier as many tools are readily available from open source web sites as opposed to highly expensive specialty diagnostic equipment used for time division multiplexing (TDM).
8. **Access and authentication**	Determine access requirements including defining users profiles, access approval criteria and validation procedures.
9. **The access any particular user has to a system is controlled through**	A series of mechanisms
10. **Accounting Management**	Usage information of network resources.
11. **The actual process of determining what is hardened and to what level varies**	Based on the risk and exposure of the system
12. **administrative and control functions**	Might be limited within network software
13. **Administrators can also limit the ways in which users can access systems by**	Set logon constraints based on the time of day, the total time logged on, the source address and unsuccessful logon attempts.
14. **Advantages of Virtualization**	Server hardware costs may decrease, Multiple OSs can share processing capacity and storage space, physical footprint decrease, single host can have multiple versions of the same OS, Application support personnel can have multiple versions of the same OS, a well-built, single access control on the host
15. **Advantages of VPN technologies which apply IPSec security standard**	Are their ubiquity, ease of use, inexpensive connectivity, and read, inquiry or copy only access
16. **Aircrack-ng**	802.11 WEP and WPA-PSK keys cracking program
17. **Allowable port numbers**	Range from 0 to 65535
18. **Although virtualization offers significant advantages**	They come with risk that an enterprise must manage effectively
19. **Although WAP supports Hypertext Markup Language (HTML) and extensible markup language (XML)**	The Wireless Markup Language (WML) language (an XML application) is designed specifically for small screens and one hand navigation without a keyboard.
20. **Another database security element**	Is controlling access to hard copy backups such as tape drives and hard disks
21. **Another important consideration for data security is**	Defining the data owner
22. **Another key user control is**	The privileges assigned to a particular user. These privileges must be carefully chosen and controlled to prevent misuse or compromise.
23. **Any VoIP device**	Is an IP device, it is vulnerable to the same types of attacks as any other IP device.
24. **Application controls**	Are controls over input, processing and output functions. They include methods to help ensure data accuracy, completeness, validity, verifiability and consistency, thus achieving data integrity and data reliability.

25. **Application controls include**	Firewalls, Encryption programs, Anti-malware programs, Spyware detection/removal programs, Biometric authentication
26. **Application controls may consist of**	Edit tests, totals, reconciliations and identification, and reporting of incorrect, missing or exception data.
27. **Application security measures**	Should be applied during the design and development phase of the application, followed by routine security countermeasures used throughout the life cycle.
28. **are reserved for certain privileged services the well-known ports**	Ports 0 to 1023
29. **Assessment scope**	Must be clearly defined and understood by everyone involved in the risk assessment process
30. **Asset**	Important assets are defined first, and then potential threats to those assets are analyzed. Vulnerabilities are identified that may be exploited to access the asset
31. **Assignment of privileges should**	Follow the principle of least privilege required for a user to do their job.
32. **Attack phase of penetration testing**	Is the process of verifying previously identified vulnerabilities by attempting to exploit them. Sometimes exploit attempts do not provide the tester with access, but they do give the tester additional information about the target and its potential vulnerabilities.
33. **Auditability**	Keep track of access, authorizations, changes and transactions.
34. **Automated controls**	Should be coupled with manual procedures to ensure proper investigation of exceptions
35. **automated tools**	Can be used to identify common vulnerabilities in computer and network implementations and configurations
36. **Availability**	Determine the uptime and downtime tolerances for different data types.
37. **Based on the risk assessment results**	A mitigation strategy can be chosen for each risk and appropriate controls and countermeasures can be designed and implemented.
38. **Because of the importance of SCADA systems**	They can be targeted by many different adversaries, and the impact of a successful attack can be catastrophic or even life threatening.
39. **Because of the key reuse problem and other flaws**	The current standardized version of WEP does not offer strong enough security for most corporate applications
40. **Because the host in a virtualized environment represents a potential single point of failure within the system**	A successful attack on the host could result in a compromise that is larger in both scope and impact
41. **Broken Authentication and Session Management**	If an application function related to authentication or session management is not implemented correctly, it can allow an attacker to compromise passwords, keys or session tokens and impersonate users.
42. **Business information belongs to**	Whoever is ultimately responsible for the business process
43. **Can have a significant impact on risk management.**	Cultural aspects like financial institutions or small entrepreneurial start-ups
44. **Classification levels**	Should be kept to a minimum and be simple designations that assign different degrees of sensitivity and criticality.
45. **The classification scheme**	Should convey the association of the data and their supporting business processes.
46. **Code review processes**	Vary from informal processes to very formal walk-throughs, team review or code inspections
47. **Common file accesses include**	Creation, modification, read, write and deletion controls
48. **Commonly available network security administrative capabilities include**	Declaring ownership of programs, files and storage, Limiting access to a read-only basis, Implementing record and file locking to prevent simultaneous update, Enforcing user ID/password sign-on procedures, Using switches, Encrypting local traffic using IPSec

49.	**Confidentiality**	Determine where sensitive data are stored and how they are transmitted.
50.	**Configuration Management**	Configuration aspects of network devices include configuration file management, inventory management and software management
51.	**The controls used to protect databases**	Should be designed in conjunction with system and application controls and form another layer of protection in a defense in depth scheme
52.	**Cross-Site Request Forgery (CSRF)**	A CSRF attack occurs when an attacker forces a user's browser to send forged HTTP requests, including session cookies. This allows an attacker to trick victims into performing operations on the illegitimate web site.
53.	**Cross-Site Scripting (XSS)**	XSS flaws occur when an application takes untrusted data and sends it to a web browser without proper validation. This is the most prevalent web application security flaw. Attackers can use XSS to hijack user sessions, insert hostile content, deface web sites and redirect users.
54.	**cyberrisk assessment**	Existing controls and other mitigation strategies are evaluated to determine the level and effectiveness of risk mitigation currently in place and identify deficiencies and gaps that require attention.
55.	**cyberrisk assessment**	Process begins with an examination of the risk sources (threats and vulnerabilities) for their positive and negative consequences.
56.	**cyberrisk assessment**	Of these attributes of risk must be analyzed to determine an organization's particular risk.
57.	**Cybersecurity professionals often use**	Command line tools as part of their security routine
58.	**Databases**	Can be individually protected with control that is similar to protections applied at the system level
59.	**Database security**	Protects stored files and information in an organization's network database
60.	**Data classification**	Should be defined in a data classification policy that provides definition of different classes of information and how each class of information should be handled and protected
61.	**Data classification**	Works by tagging data with metadata based on a classification taxonomy. This enables data to be found quickly and efficiently, cuts back on storage and backup costs and helps to allocate and maximize resources
62.	**The data owner**	May be an individual who creates the data or an organizational element that acts as a custodian of the information.
63.	**The data owner**	Is usually responsible for determining the data classification and therefore the level of protection required
64.	**Data retention**	Determine retention periods and preserve specific versions of software, hardware, authentication credentials and encryption keys to ensure availability.
65.	**Decentralized local processing**	Provides the potential for a more responsive computing environment; however, organizations do not always give the opportunity to efficiently develop staff to address the technical, operational and control issues that the complex LAN technology represents
66.	**The design and deployment of controls will often be undertaken**	As a systems development project
67.	**Development and testing environments**	Are relatively open and often have fewer access controls due to the collaborative nature of the development process
68.	**Different access controls (credentials)**	Should be used between the different environments
69.	**Disadvantages of Virtualization**	Inadequate configuration of the host could create vulnerabilities that affect not only the host, Exploits of vulnerabilities within the host's configuration, grant unapproved administrative access to the host's guests, Performance issues, data leak, Insecure protocols for remote access

70. **Disadvantages of VPN technologies which apply IPSec security standard**	Include that they are significantly less reliable than dedicated circuits, lack a central authority, and can be difficult to troubleshoot
71. **Discovery phase of penetration testing**	The penetration tester gathers information by conducting research on the organization and scans the networks for port and service identification.
72. **Distractions caused by the devices**	The use of wireless devices distract the user. If these devices are being used in situations where an individual's full attention is required (e.g., driving a car), they could result in an increase in the number of accidents.
73. **DoS, or the flooding of the data network with data**	Is a common issue in the protection of data networks but needs to be revisited as quality of service (QoS) becomes implemented for VoIP networks
74. **The dynamic and/or private ports**	49152 through 65535
75. **Each year, OWASP publishes a list of**	The top 10 application security risks
76. **Emergent Vulnerability**	Interactions between, or changes in, environments like Cross-organizational failures, Interoperability errors, Implementing new technology
77. **The emphasis has been on providing capability and functionality rather than**	Security
78. **Encrypted VPN traffic can**	Hide unauthorized actions or malicious software that can be transmitted through such channels
79. **Examples of common security events include**	Authentication failures (incorrect passwords) and logging of accesses to critical system files
80. **Examples of specialized systems include**	Supervisory control and data acquisition (SCADA) systems or other real-time monitoring or control systems that operate in specialized environments
81. **exploit.**	Method used to take advantage of a vulnerability
82. **failure to planning penetration testing**	May result in ineffective results, negative impact on or damage to the organization's IT infrastructure or potential liability or criminal prosecution
83. **Fault Management**	Detect, isolate, notify and correct faults encountered in the network. This category analyzes traffic, trends, SMMP polls and alarms for automatic fault detection.
84. **File security**	Wireless phones and PDAs do not use the type of file access security that other computer platforms can provide.
85. **For TCP, UDP and ICMP**	A port number is a 16-bit integer that is put in the header attached to a unit of information then passed logically between client and server transport layers and physically between the transport layer and the Internet protocol layer and then forwarded.
86. **For the risk assessment to be successful**	The risk assessment process should fit the goals of the organization, adequately address the environment being assessed and use assessment methodologies that fit the data that can be collected
87. **General issues and exposures related to wireless access**	The interception of sensitive information, The loss or theft of devices, The misuse of devices, Distractions caused by the devices, Possible health effects of device usage, Wireless user authentication, File security, WEP security encryption, nteroperability, Translation point
88. **A good practice will terminate all VPNs to the same end point**	A so called VPN concentrator, and will not accept VPNs directed at other parts of the network.
89. **Higher-level applications that use TCP/IP like**	Web protocol and hypertext transfer protocol (HTTP) use ports with preassigned numbers
90. **identify and assess vulnerabilities**	To determine the threat and potential impact and to determine the best course of action in addressing each vulnerability.
91. **IEEE 802.11's Wired Equivalent Privacy (WEP) encryption**	Uses symmetric, private keys, which means the end user's radio-based NIC and access point must have the same key

92.	**if production data are used in the test environment**	Private or personally identifiable information should be scrambled so that confidential information is not inadvertently disclosed
93.	**If risk is not properly analyzed**	The implementation of security is left to guesswork.
94.	**Implementation of these automated controls**	Helps ensure system integrity, that applicable system functions operate as intended, and that information contained by the system is relevant, reliable, secure and available when needed.
95.	**The information an organization uses**	Can be of varying value and importance
96.	**Information may also need to be**	Reclassified based on changes to its importance
97.	**Information used to estimate impact and likelihood usually comes from**	Past experience or data and records, Reliable practices, international standards or guidelines, Market research and analysis, Experiments and prototypes, Economic, engineering or other models, Specialist and expert advice
98.	**Injection**	Injection flaws occur when untrusted data is sent to an interpreter. The attacker can trick the interpreter into executing unintended commands or accessing unauthorized data. Injection flaws are prevalent and are often found in SQL and LDAP queries and OS commands.
99.	**In order to reduce application security risk, OWASP recommends the following:**	Define application security requirements, Utilize good application security architecture practices, Build strong and usable security controls, Integrate security into the development lifecycle, Stay current on application vulnerabilities
100.	**Insecure applications**	Open your organization up to external attackers who may try to use unauthorized code to manipulate the application to access, steal, modify or delete sensitive data
101.	**Insecure Direct Object References**	A direct object reference occurs when a developer exposes a reference to an internal implementation object. Attackers can manipulate these references to access unauthorized data.
102.	**Integrity**	Protect data from unauthorized changes using change control procedures and automated monitoring and detection for unauthorized changes and manipulation.
103.	**The interception of sensitive information**	Information is transmitted through the air, which increases the potential for unprotected information to be intercepted by unauthorized individuals.
104.	**Interoperability**	Most vendors offer 128-bit encryption modes. they are not standardized, so there is no guarantee that they will interoperate. The use of the 128-bit encryption key has a major impact on performance with 15-20 percent degradation being experienced.
105.	**Intrusion detection systems (IDSs) and virus scanners**	Are able to decrypt the traffic for analysis and then encrypt and forward it to the VPN end point should be considered as preventive controls
106.	**The IP end point**	Is often overlooked, but it can be singled out as a point of attack and flooded with data, causing the device to reboot and eventually become unusable
107.	**(ISO) network management model defines five functional areas of network management (FCAPS):**	Fault Management, Configuration Management, Accounting Management, Performance Management, Security Management
108.	**Is only becoming standard now**	The use of logon IDs and passwords with associated administration facilities
109.	**It is common for most computer vendors**	To set the default controls to be open, allowing ease of use over security. This creates significant vulnerabilities unless the system is hardened.
110.	**It is important for an organization to understand**	The sensitivity of information and classify data based on its sensitivity and the impact of release or loss of the information.

111.	**It is important to analyze vulnerabilities in the context of**	How they are exploited, and both vulnerabilities and exploits need to be considered in vulnerability assessments.
112.	**It is important to separate the development, testing and production environments**	To minimize a compromise or misconfiguration being introduced or cascading through the process
113.	**John the Ripper**	Password cracker
114.	**kernel mode**	For execution of privileged instructions for the internal operation of the system. there are no protections from errors or malicious activity and all parts of the system and memory are accessible
115.	**These kinds of devices that use displays and access the Internet run what are called**	Micro-browsers, which have small file sizes that can accommodate the low-memory constraints of hand held devices and the low-bandwidth constraints of a wireless hand held network
116.	**Kismet**	02.11 layer 2 wireless network detector, sniffer and IDS
117.	**LANs**	Facilitate the storage and retrieval of programs and data used by a group of people.
118.	**LANs**	Can represent a form of decentralized computing.
119.	**LANs and WANs**	Are particularly susceptible to people and virus-related threats because of the large number of people who have access rights.
120.	**LAN software and practices**	Also need to provide for the security of these programs and data
121.	**Layer 2 tunneling protocol (L2TP)**	A protocol that encapsulates point-to-point protocol data and is compatible among different manufacturers' equipment. The end points do not have to reside on the same packet-switched network and can remain isolated from other traffic.
122.	**local LAN administrators**	Frequently lack the experience, expertise and time to effectively manage the computing environment.
123.	**local regulations**	May impact data classification and handling such as those controlled by data protection acts
124.	**Logging**	Provides the basic data required to monitor and detect unauthorized activity and to analyze potential security breaches
125.	**Logging too little activity**	Will not provide adequate information to detect attacks
126.	**Logging too much activity can**	Make anaylsis difficult, as well as waste resources such as the disk space to store the activity
127.	**The loss or theft of devices**	Wireless devices tend to be relatively small, making them much easier to steal or lose. If encryption is not strong, a hacker can easily get at the information that is password- or PIN-protected. Theft or loss can result in the loss of data that have been stored on these devices.
128.	**Many existing SCADA systems did not**	Consider security in their design or deployment, and while vendors are improving security, these systems require careful assessment of risk and threats and often require special controls to compensate for inherent weaknesses.
129.	**Many security teams**	Spend most of their time preventing outside attackers from penetrating a corporate firewall or Internet-accessible bastion servers
130.	**Metasploit**	Penetration testing software
131.	**Meterpreter**	Metasploit's most popular payload which enables a user to upload and download files from the system, take screenshots and collect password hashes.
132.	**Missing Function Level Access Control**	When function level access rights are not verified, attackers can forge requests to access functionality without authorization.
133.	**The misuse of devices**	Devices can be used to gather information or intercept information that is being passed over wireless networks for financial or personal benefit
134.	**Most attacks seek to gain**	Privileged or kernel mode access to the system in order to circumvent other security controls.
135.	**most LAN software**	Provides a low level of security

136. **Most operating systems have a wide range of events and transactions that can be**	Recorded and stored for troubleshooting, performance and security monitoring
137. **Most operating systems have two modes of operations**	Kernel mode and user mode
138. **Most operating systems provide controls around passwords such as**	Minimum length, lifetime for any particular password and how many attempts to use a password are allowed before denying access.
139. **The most useful standard used**	Is the IEEE 802.11 standard.
140. **Netcat**	Networking utility that reads and writes data across network connections, using the TCP/IP protocol
141. **Netstat**	Displays detailed network status information
142. **Network administration**	Is often inadequate, providing global access because of the limited administrative support available when limited access is appropriate
143. **Network management**	Is the process of assessing, monitoring, and maintaining network devices and connections.
144. **Newer security protocols such as 802.11i WPA2 and Wi-Fi Protected Access (WPA)**	Utilize public key cryptography techniques to provide effective authentication and encryption between users and access points
145. **newer versions of network software**	Have significantly more control and administration capabilities.
146. **Nmap**	Network port scanner and service detector
147. **No organization is static**	Technology, business, regulatory and statutory requirements, people, vulnerabilities and threats are continuously evolving and changing.
148. **Not considering the security in the design of a system or application**	Is one of the major contributing factors to today's cybersecurity vulnerabilities, making it easier for systems to be compromised
149. **Once data classification has been assigned**	Security controls can be established such as encryption, authentication and logging. Security measures should increase as the level of data sensitivity or criticality increases.
150. **Once risk is identified and prioritized**	Existing controls should be analyzed to determine their effectiveness in mitigating the risk. This analysis will result in a final risk ranking based on risk that has adequate controls, inadequate controls and no controls.
151. **Once vulnerabilities are identified and assessed**	Appropriate remediation can take place to mitigate or eliminate the vulnerability
152. **One of the best ways to secure stored files and information information is**	With the digital rights management (DRM), which refers to access control technologies that can be used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices
153. **OpenSSH/PuTTY/SSH**	Program for logging into or executing commands on a remote machine
154. **The Open Web Application Security Project (OWASP)**	Is an open community dedicated to application security
155. **Operating systems allow controlled access to kernel mode operations through**	System calls that usually require privileges. These privileges are defined on a user or program basis and should be limited under the principle of least privilege.
156. **Operating systems have**	File systems that manage data files stored within the system and provide access controls to determine which users (or programs) have what type of access to a file
157. **Organizational Vulnerability**	Errors in management, decision, planning or from ignorance like Lack of policies, Lack of awareness, Failure to implement controls
158. **Organizations can also restrict access to specific instances of**	Digital works or devices.

159.	**Organizations often commit significant**	Resources (e.g., people, applications, facilities and technology) to develop, acquire, integrate and maintain application systems that are critical to the effective functioning of key business processes.
160.	**Organizations should be aware that using VPNs to allow remote access to their systems**	Can create holes in their security infrastructure
161.	**Other vulnerability analysis tools**	Open source and proprietary sources such as SANS, MITRE and OWASP, software vendors, historical incidents, etc.
162.	**Ownership and distribution**	Establish procedures to protect data from unauthorized copy and distribution.
163.	**Passwords**	Are the standard mechanism to authenticate a user to the system and must be managed correctly to ensure they are not easily guessed or compromised
164.	**A payload**	Is typically attached to and delivered by the exploit
165.	**A payload**	Is the piece of software that lets a user control a computer system after it has been exploited
166.	**Penetration testing**	Should not be performed by untrained or unqualified practitioners.
167.	**Penetration testing**	Requires specialized knowledge of vulnerabilities, exploits, IT technology and the use of testing tools.
168.	**Penetration testing**	Can be external, from outside the organization, or internal, starting from a system behind the organization's firewall.
169.	**Penetration testing**	Should be carefully planned to mitigate the risk of causing a service outage, and the results require careful interpretation and elimination of false positives
170.	**Penetration testing**	Can be covert (the general IT staff do not know the testing is going to take place) so that the reactions of the organization to detect and respond are also tested
171.	**Penetration testing**	Includes identifying existing vulnerabilities and then using common exploit methods
172.	**penetration testing**	Ensure testers implement "Do no harm" procedures to ensure no assets are harmed, such as deletions, denial-of-service (DoS) or other negative impacts.
173.	**penetration testing**	Simulates actual attacks, it is important to plan these tests carefully.
174.	**penetration testing**	Clearly define the scope of the test including what systems or networks are within and out of scope, the type of exploits that may be used and the level of access allowed. These exploits can include network, social engineering, web, mobile application and other kinds of testing.
175.	**penetration testing**	Gather explicit, written permission from the organization authorizing the testing. This is the only accepted industry standard that distinguishes the service as authorized and legal.
176.	**penetration testing**	Put in place communication and escalation plans for the organization and testers to communicate quickly during the tests.
177.	**Performance Management**	Monitor and measure various aspects of performance metrics so that acceptable performance can be maintained. This includes response time, link utilization and error rates. Administrators can monitor trends and set threshold alarms.
178.	**Planning phase of penetration testing**	The goals are set, the scope is defined and the test is approved and documented by management. The scope determines if the penetration test is internal or external, limited to certain types of attacks or limited to certain networks or assets.
179.	**Point-to-point tunneling protocol (PPTP)**	A Layer 2 protocol developed by Microsoft that encapsulates point-to-point protocol data. It is simple, but less secure than other tunneling protocols
180.	**A port**	Is a logical connection.
181.	**Port 7**	Echo - TCP/UDP
182.	**Port 19**	chargen - TCP
183.	**Port 20-21**	FTP - TCP
184.	**Port 23**	Telnet - TCP
185.	**Port 25**	STMP - TCP
186.	**Port 43**	Whois- TCP/UDP
187.	**Port 53**	DNS - TCP
188.	**Port 69**	TFTP - UDP
189.	**Port 79**	Finger - TCP

190.	**Port 80**	HTTP-low - TCP
191.	**Port 107**	Rtelnet- TCP/UDP
192.	**Port 110**	POP3 - TCP
193.	**Port 111/2049**	SunRPC- TCP/UDP
194.	**Port 135-139**	NetBIOS- TCP/UDP
195.	**Port 161, 162**	SNMP - UDP
196.	**Port 512**	Exec - UDP
197.	**Port 513**	Login - TCP
198.	**Port 514**	Shell- TCP/UDP
199.	**Port 6000-xxxx**	X-Windows - TCP
200.	**a port number**	Is a way to identify the specific process to which an Internet or other network message is to be forwarded when it arrives at a server
201.	**Port numbers are divided into three ranges**	The well-known ports, the registered ports and the dynamic and/or private
202.	**Port scanning**	Is often a precursor to a potential sniffing of the VoIP network
203.	**Possible health effects of device usage**	The safety or health hazards have not yet been identified. However, there are currently a number of concerns with respect to electromagnetic radiation, especially for those devices that must be held beside the head.
204.	**The principal advantages of standards**	Encourage mass production and to allow products from multiple vendors to interoperate
205.	**prior to a product release**	Details of the design, pricing and other information may be confidential and need significant protection; however, after the product is announced, this information may become public and not require the same levels of protection.
206.	**Privacy**	Utilize controls to warn an affected user that his or her information is about to be used.
207.	**Process Vulnerability**	Errors in operation like Failure to monitor logs, Failure to patch software
208.	**Read, write and execute permission**	These capabilities for files and programs are options available with some network operating system versions, but detailed automated logs of activity (audit trails) are seldom found on LANs
209.	**Regardless of the specific operating system**	System hardening should implement the principle of least privilege or access control
210.	**The registered ports**	1024 through 49151
211.	**remediation**	Will be through a patch management process but may also require reconfiguration of existing controls or addition of new controls.
212.	**Remote access controls include**	Policies and standards, Proper authorizations, Identification and authentication mechanisms, Encryption tools and techniques such as use of a VPN, System and network management
213.	**Remote access risk include**	DoS, Malicious third parties, Misconfigured communications software, Misconfigured devices on the corporate computing infrastructure, Host systems not secured appropriately, Physical security issues over remote users' computers
214.	**Remote access users**	Can connect to their organization's networks with the same level of functionality that exists within their office
215.	**Reporting phase of penetration testing**	Occurs simultaneously with the other phases. An assessment plan is developed during the planning phase. Logs are kept during the discovery and attack phases at the conclusion of the penetration test, a report is developed to describe the vulnerabilities identified, assign risk ratings and provide mitigation plans.
216.	**risk**	Is defined as the possibility of loss of a digital asset resulting from a threat exploiting a vulnerability
217.	**risk**	Can be ranked according to likelihood and impact
218.	**Risk Acceptance**	If the risk is within the organization's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, then an organization can assume the risk and absorb any losses.
219.	**risk analyses**	Can be oriented toward one of the inputs, making the risk assessment asset-oriented, threat-oriented or vulnerability-oriented

220.	**risk assessment**	Is not a one-off process.
221.	**risk assessment methodology inputs**	Asset identification, threat assessment and vulnerability assessment
222.	**Risk assessment results**	Can also be used to communicate the risk decisions and expectations of management throughout the organization through policies and procedures.
223.	**Risk Assessments**	Can be used to identify areas where incident response capabilities need to be developed to quickly detect and respond to inherent or residual risk or where security controls cannot adequately address the threat
224.	**risk assessments**	Some organizations will perform these from more than one orientation to compensate for the potential bias and generate a more thorough analysis.
225.	**risk assessments results**	Need to be evaluated in terms of the organization's mission, risk tolerance, budgets and other resources, and cost of mitigation
226.	**risk associated with use of LANs includes**	Improper disclosure of data, Violation of software licenses, Illegal access, Internal user's sniffing, Internal user's spoofing, Destruction of the logging and auditing data
227.	**risk associated with use of LANs includes**	Loss of data and program integrity, Lack of current data protection, Exposure to external activity, Virus and worm infection
228.	**Risk Avoidance**	Risk can be avoided by not participating in an activity or business.
229.	**Risk Reduction**	The implementation of controls or countermeasures to reduce the likelihood or impact of a risk to a level within the organization's risk tolerance.
230.	**Risk response strategy**	Depends on many different things such as regulatory requirements, culture, mission, ability to mitigate risk and risk tolerance
231.	**Risk Transfer or Sharing**	Risk can be transferred to a third party (e.g., insurance) or shared with a third party via contractual agreement
232.	**SCADA systems**	These systems are not commonly networked and often have few of the common controls found in more commercial systems.
233.	**SCADA systems**	Were designed as stand-alone systems and because of the real-time nature of their applications often did not have any "overhead" software that would slow down operations.
234.	**SCADA systems**	Control industrial and manufacturing processes, power generation, air traffic control systems, and emergency communications and defense systems.
235.	**scheduled downtime in telephony**	Doesn't exist
236.	**The SDLC design requirements that include**	Business requirements (what system should do), Functional requirements (how users will interact), Technical requirements (design/coding specifics) Risk mitigation and control requirements (to protect integrity of system)
237.	**The SDLC includes**	IT processes for managing and controlling project activity, An objective for each phase of the life cycle that is typically described with key deliverables, a description of recommended tasks and a summary of related control objectives for effective management, Incremental steps or deliverables
238.	**The SDLC process**	Guides the phases deployed in the development or acquisition of a software system and, depending on the methodology, may even include the controlled retirement of the system.
239.	**The SDLC requirements**	Is a formal process to characterize design requirements
240.	**Security and risk mitigation**	Should be formal design criteria in any SDLC process and start with threat and risk assessment of the proposed system, identification of controls, implementation of those controls, and testing and review
241.	**Security Management**	Provide access to network devices and corporate resources to authorized individuals. This category focuses on authentication, authorization, firewalls, network segmentation, IDS and notifications of attempted breaches.

242.	**Security Misconfiguration**	Security settings must be defined, implemented and maintained for applications, frameworks, application servers, web servers, database servers and platforms. Security misconfiguration can give attackers unauthorized access to system data or functionality.
243.	**Security should be an integrated part of**	Any review process
244.	**Sensitive Data Exposure**	If web applications do not properly secure sensitive data through the use of encryption, attackers may steal or modify sensitive data such as health records, credit cards, tax IDs and authentication credentials.
245.	**Sniffing**	Would allow the disclosure of sensitive information, such as user information, resulting in identity theft, which may be used to attack other data subsystems.
246.	**Snort**	Open source IDS/IPS
247.	**Software vendors and network users**	Have recognized the need to provide diagnostic capabilities to identify the cause of problems when the network goes down or functions in an unusual manner.
248.	**some common hardening controls include**	Authentication and authorization, File system permissions, Access privileges, Logging and system monitoring, System services
249.	**some information may be public and require minimal protection while other information such as**	National security information, health or other personal information or trade secrets could result in significant harm to the organization if inadvertently released, deleted or modified.
250.	**Specific controls that can be placed at the database level include**	Authentication and authorization of access, Access controls limiting or controlling the type of data that can be accessed and what types of accesses are allowed, Logging and other transactional monitoring, Encryption and integrity controls, Backups
251.	**Static WEP**	Is a serious security risk, as a static key can easily be lost or broken, and, once this has occurred, all of the information is available for viewing and use. An attacker possessing the WEP key could also sniff packets being transmitted and decrypt them.
252.	**successful risk assessment**	Is an ongoing process to identify new risk and changes to the characteristics of existing and known risk.
253.	**System Hardening**	Is the process of implementing security controls on a computer system
254.	**Takes considerable planning and knowledge of specific risk assessment methodologies**	Choosing the exact method of analysis, including qualitative or quantitative approaches and determining the analysis orientation
255.	**Tape management systems (TMS) and disk management systems (DMS)**	Often include physical security procedures that guard access to backup machines as well as inventory control systems to account for database backups.
256.	**Tcpdump**	Command line packet analyzer
257.	**TCP/IP designating a port**	Is the way a client program specifies a particular server program on a computer in a network
258.	**TCP/IP Internet-based remote access**	Is a cost effective approach that enables organizations to take advantage of the public network infrastructures and connectivity options available, under which ISPs manage modems and dial-in servers, and DSL and cable modems reduce costs further to an organization
259.	**Technical Vulnerability**	Errors in design, implementation, placement or configuration like Coding errors, Inadequate passwords, Open network ports, Lack of monitoring
260.	**Techniques used to gather information in the Discovery phase of penetration testing include**	DNS interrogation, WHOIS queries and network sniffing, Search web servers and directory servers, Banner grabbing for application and service information, NetBIOS enumeration for system information, Dumpster diving and physical walk-throughs, Social engineering

261.	**ten popular command line tools for cybersecurity**	Nmap, Metasploit, Aircrack-ng, Snort, Netstat, Tcpdump, John the Ripper, Kismet, OpenSSH/PuTTY/SSH
262.	**testing phase of SDLC includes**	A program, subsystem or application, and the designed security controls perform the functions for which they have been designed, Determination of whether the units being tested operate without any malfunction or adverse effect on other components of the system, A variety of development methodologies and organizational requirements
263.	**Threat**	Potential threats are determined first, and then threat scenarios are developed. Based on the scenarios, vulnerabilities and assets of interest to the adversary are determined in relation to the threat
264.	**To address VM risk as a single point of failure**	Strong physical and logical access controls, Sound configuration management practices and system hardening for the host, Appropriate network segregation, Strong change management practices
265.	**To address VM risk as a single point of failure**	An enterprise can often implement and adapt the same principles and best practices for a virtualized server environment that it would use for a server farm
266.	**To effectively use TCP/IP Internet-based remote access**	Organizations establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure.
267.	**Too often, security is an afterthought**	and controls are retrofitted in an ad hoc way only after security weaknesses are identified
268.	**tracking vulnerabilities and the remediation efforts to mitigate them**	Provides a clear opportunity to provide good qualitative metrics to the organization's management on the numbers and types of vulnerabilities, the potential impacts and the effort needed to mitigate them.
269.	**Traffic flow disruption**	Allows further exploitation of the previous two vulnerabilities, whereas the redirecting of packets facilitates the determination of packet routes, increasing the likelihood of sniffing
270.	**Translation point**	The location where information being transmitted via the wireless network is converted to the wired network. The information is converted to the secure socket layer, where the information is decrypted and then encrypted again for communication via TCP/IP.
271.	**Tunneling**	Transports higher-layer data over a VPN by Layer 2 protocols
272.	**Tunneling**	Is the process of encapsulating one type of protocol in another
273.	**Two common types of tunneling include**	Point-to-point tunneling protocol (PPTP) and Layer 2 tunneling protocol (L2TP)
274.	**two most common vulnerability techniques**	Scanning and penetration testing
275.	**understanding the cybersecurity assets and where they reside**	By maintaining an asset inventory that details important information about each cyberasset such as location (physical or logical), criticality of the asset, the organizational owner of the asset and the type of information the asset stores or processes.
276.	**Unless network-based encryption is used**	All voice RTP packets travel in the clear over the network and could be captured or copied by any network-monitoring device
277.	**Unvalidated Redirects and Forwards**	Web applications frequently redirect or forward users to other pages. When untrusted data are used to determine the destination, an attacker can redirect victims to phishing or malware sites.
278.	**user mode**	For normal activities
279.	**Users are only given access to**	The files they need to prevent internal attacks and attacks that dupe employees into providing secure data.
280.	**A user's credentials define**	Who they are and what permissions they have to access resources within the system

281.	**Using common exploit methods with penetration testing to**	Confirm exposures, Assess the level of effectiveness and quality of existing security controls, Identify how specific vulnerabilities expose IT resources and assets, Ensure compliance
282.	**Using Components with Known Vulnerabilities**	Certain components such as libraries, frameworks and other software modules usually run with full privileges. Attackers can exploit a vulnerable component to access data or take over a server.
283.	**US Sarbanes-Oxley Act**	Defines which data records must be stored and for how long.
284.	**A very important criterion in control selection and evaluation**	Is that the cost of the control (including its operation) should not exceed value of the asset it is protecting.
285.	**A viable Remote access option gaining increased use**	TCP/IP Internet-based remote access
286.	**Virtualization**	Creates a layer between the hardware and the guest OSs to manage shared processing and memory resources on the host
287.	**Virtualization**	Allows multiple OSs (guests), to coexist on the same physical server (host), in isolation of one another.
288.	**Virtualization**	Provides an enterprise with a significant opportunity to increase efficiency and decrease costs in its IT operations.
289.	**voice communications**	Users often expect they are confidential
290.	**Voice packets**	Travel "in the clear" over IP networks, so they may be vulnerable to unauthorized sniffing
291.	**VoIP networks**	Are still vulnerable to sniffing, DoS, traffic-flow disruption and toll fraud
292.	**VoIP networks**	Have a number of characteristics that make for special security requirements
293.	**VoIP outages**	May result in massive, widespread customer panic or outrage. There could also be disclosure of confidential information, which, like the loss of other kinds of data, could adversely affect the organization
294.	**Vulnerabilities**	Are continuously being discovered and organizations must be constantly vigilant in identifying them and quickly remediating
295.	**Vulnerabilities**	Can occur in many different forms and at different architectural levels (for example, physical, operating system, application).
296.	**Vulnerabilities can be identified by**	Information provided by software vendors (e.g., through the release of patches and updates) and by utilizing processes and tools that identify known vulnerabilities in the organization's specific environment
297.	**Vulnerability**	Vulnerabilities and deficiencies are identified first, then the exposed assets, and then the threat events that could be taken advantage of are determined.
298.	**vulnerability**	An exploitable weakness that results in a loss
299.	**Vulnerability management**	Starts by understanding the cybersecurity assets and where they reside—both physically and logically.
300.	**Vulnerability management**	Includes tracking vulnerabilities and the remediation efforts to mitigate them
301.	**Vulnerability scanning**	Is the process of using proprietary or open source tools to search for known vulnerabilities
302.	**Vulnerability scans**	Conducted regularly to identify new vulnerabilities and ensure previously identified vulnerabilities have been properly corrected.
303.	**WAP**	Supports most wireless networks and is supported by all operating systems specifically engineered for handheld devices and some mobile phones
304.	**WAP protocols**	Are largely based on Internet technologies. The motivation for developing WAP was to extend Internet technologies to wireless networks and devices.
305.	**well known ports**	To which numbers have been assigned by the Internet Assigned Numbers Authority (IANA)
306.	**The well-known ports**	0 through 1023
307.	**WEP**	Leads to periodic difficulties distributing new keys to each NIC and keys remain unchanged on networks for extended times.

308.	**WEP security encryption**	WEP security depends particularly on the length of the encryption key and on the usage of static WEP or dynamic WEP. The 64-bit encryption keys that are in use in the WEP standard encryption can be easily broken
309.	**When classifying data, the following requirements should be considered**	Access and authentication, Confidentiality, Privacy, Availability, Ownership and distribution, Integrity, Data retention, Auditability
310.	**When designing a VPN**	It is important to ensure that the VPN can carry all types of data in a secure and private manner over any type of connection.
311.	**When performing a risk assessment**	It is important to understand the organization's unique risk appetite and cultural considerations
312.	**While there are several project management techniques that can be used to manage system development projects**	They should be an integral and equal part of any SDLC process
313.	**Wireless Application Protocol (WAP)**	Is a general term used to describe the multilayered protocol and related technologies that bring Internet content to wireless mobile devices such as smartphones
314.	**Wireless user authentication**	There is a need for stronger wireless user authentication and authorization tools at the device level. The current technology is just emerging.
315.	**With static WEP keys**	Several hacking tools easily break through the relatively weak WEP encryption mechanisms.
316.	**WLAN technologies**	Conform to a variety of standards and offer varying levels of security features