CompTIA Security+ Practice Questions

**Question 1.**  
  
Which of the following BEST describes both change and incident management?

a) Incident management is not a valid term in IT, however change management is  
b) Change management is not a valid term in IT, however incident management is  
c) Incident management and change management are interchangeable terms meaning the same thing  
d) Incident management is for unexpected consequences, change management is for planned work

**Question 2.**  
  
Which of the following account policy controls requires a user to enter a 15 character alpha-numerical password?

a) Disablement  
b) Length  
c) Expiration  
d) Password complexity

**Question 3.**  
  
Which of the following information types would be considered personally identifiable information?

a) First name and home address  
b) Social security number  
c) Date of birth  
d) Full name, date of birth and address

**Question 4.**  
  
Which of the following is the benefit of single file versus full disk encryption?

a) Encryption is preserved in full disk encryption when a file is copied from one media to another  
b) Encryption is preserved in single file encryption when a file is copied from one media to another  
c) Single file encryption provides better security when decrypting single files than full disk encryption when properly implemented and used  
d) Full disk encryption provides better security when decrypting single files than single file encryption when properly implemented and used

**Question 5.**  
  
Which of the following is another name for a CAC?

a) Token  
b) RFID  
c) MAC  
d) PIV

**Question 6.**  
  
Which of the following systems offers Trusted OS capabilities by default?

a) Windows Vista  
b) Windows 7  
c) SE Linux  
d) Backtrack

**Question 7.**  
  
Which of the following describes a common operational problem when using patch management software that results in a false sense of security?

a) Conflicts with vulnerability scans impede patch effectiveness  
b) Distributed updates may fail to apply or may not be active until a reboot  
c) Vendor patches are released too frequently consuming excessive network bandwidth  
d) It is resource intensive to test all patches

**Question 8.**  
  
Which of the following is BEST identified as an attacker who has or is about to use a Logic bomb?

a) Grey hat  
b) Malicious insider  
c) White hat  
d) Black box

**Question 9.**  
  
Which of the following is the BEST choice in regards to training staff members on dealing with PII?

a) PII requires public access but must be flagged as confidential  
b) PII data breaches are always the result of negligent staff and punishable by law  
c) PII must be handled properly in order to minimize security breaches and mishandling  
d) PII must be stored in an encrypted fashion and only printed on shared printers

**Question 10.**  
  
Which of the following processes are used to avoid employee exhaustion and implement a system of checks and balances?

a) Job rotation  
b) Incident response  
c) Least privilege  
d) On-going security

**Question 11.**  
  
When designing secure LDAP compliant applications, null passwords should NOT be allowed because:

a) null password can be changed by all users on a network  
b) a null password is a successful anonymous bind  
c) null passwords can only be changed by the administrator  
d) LDAP passwords are one-way encrypted

**Question 12.**  
  
A security administrator visits a remote data center dressed as a delivery person. Which of the following is MOST likely being conducted?

a) Social engineering  
b) Remote access  
c) Vulnerability scan  
d) Trojan horse

**Question 13.**  
  
Mobile devices used in the enterprise should be administered using:

a) encrypted networks and system logging  
b) full disk encryption and central password management  
c) vendor provided software update systems  
d) centrally managed update services and access controls

**Question 14.**  
  
The Chief Information Officer (CIO) wants to implement widespread network and hardware changes within the organization. The CIO has adopted an aggressive deployment schedule and does not want to bother with documentation, because it will slow down the deployment. Which of the following are the risks associated with not documenting the changes?

a) Undocumented networks might not be protected and can be used to support insider attacks  
b) Documenting a network hinders production because it is time consuming and ties up critical resources  
c) Documented networks provide a visual representation of the network for an attacker to exploit  
d) Undocumented networks ensure the confidentiality and secrecy of the network topology

**Question 15.**  
  
Which of the following could mitigate shoulder surfing?

a) Privacy screens  
b) Hashing  
c) Man traps  
d) Screen locks

**Question 16.**  
  
Which of the following passwords is the MOST complex?

a) 5@rAru99  
b) CarL8241g  
c) j1l!1b5  
d) l@ur0

**Question 17.**  
  
Which of the following is being utilized when the BIOS and operating system’s responsibility is platform integrity?

a) SSL  
b) USB encryption  
c) Data loss prevention  
d) TPM

**Question 18.**  
  
Which of the following BEST describes a Buffer Overflow attack that allows access to a remote system?

a) The attacker attempts to have the receiving server run a payload using programming commonly found on web servers  
b) The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage  
c) The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information  
d) The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload

**Question 19.**  
  
A company fails to monitor and maintain the HVAC system in the datacenter. Which of the following is the MOST likely to affect availability of systems?

a) Employee productivity in a hot datacenter  
b) Premature failure of components  
c) Decreased number of systems in the datacenter  
d) Increased utility costs

**Question 20.**  
  
Which of the following protocols is defined in RFC 1157 as utilizing UDP ports 161 and 162?

a) SNMP  
b) IPSec  
c) SSL  
d) TLS

**Question 21.**  
  
Which of the following is LEAST likely to have a legitimate business purpose?

a) Metasploit  
b) Vulnerability scanner  
c) Steganography  
d) Port scanner

**Question 22.**  
  
Which of the following does full disk encryption on a laptop computer NOT protect against?

a) Confidentiality of the data  
b) Key loggers  
c) Theft of the data  
d) Disclosure of the data

**Question 23.**  
  
Which of the following passwords exemplifies the STRONGEST complexity?

a) Passw0rd  
b) P@ssw0rd  
c) Passwrd  
d) passwordpassword

**Question 24.**  
  
Which following port ranges would give a technician the MOST comprehensive port scan of a server?

a) 1024-15000  
b) 0-99999  
c) 0-65535  
d) 0-1024

**Question 25.**  
  
Which of the following attacks steals contacts from a mobile device?

a) Bluesnarfing  
b) Smurf attack  
c) Session hijacking  
d) Bluejacking

**Question 26.**  
  
Which of the following attacks sends unwanted messages to a mobile device?

a) Session hijacking  
b) Smurf attack  
c) Bluejacking  
d) Bluesnarfing

**Question 27.**  
  
A smurf attack relies on which protocol to perform a Denial of Service?

a) DNS  
b) SNMP  
c) SMTP  
d) ICMP

**Question 28.**  
  
Which of the following allows for multiple operating systems to run on a single piece of hardware?

a) Virtualization  
b) Port security  
c) Remote access  
d) DMZ

**Question 29.**  
  
A user name is an example of which of the following?

a) Identification  
b) Authentication  
c) Authorization  
d) Access

**Question 30.**  
  
The CRL contains a list of:

a) private keys  
b) public keys  
c) root certificates  
d) valid certificates

CompTIA Security+ Practice Question Answers

**Question 1.**  
  
**Objective: Carry out appropriate risk mitigation strategies**.  
  
Which of the following BEST describes both change and incident management?

a) Incident management is not a valid term in IT, however change management is  
b) Change management is not a valid term in IT, however incident management is  
c) Incident management and change management are interchangeable terms meaning the same thing  
**d) Incident management is for unexpected consequences, change management is for planned work**

**Question 2.**  
  
**Objective: Implement appropriate security controls when performing account management**.  
  
Which of the following account policy controls requires a user to enter a 15 character alpha-numerical password?

a) Disablement  
b) Length  
c) Expiration  
**d) Password complexity**

**Question 3.**  
  
**Objective: Implement appropriate security controls when performing account management**.  
  
Which of the following information types would be considered personally identifiable information?

a) First name and home address  
b) Social security number  
c) Date of birth  
**d) Full name, date of birth and address**

**Question 4.**  
  
**Objective: Explain the importance of data security**.  
  
Which of the following is the benefit of single file versus full disk encryption?

a) Encryption is preserved in full disk encryption when a file is copied from one media to another  
**b) Encryption is preserved in single file encryption when a file is copied from one media to another**  
c) Single file encryption provides better security when decrypting single files than full disk encryption when properly implemented and used  
d) Full disk encryption provides better security when decrypting single files than single file encryption when properly implemented and used

**Question 5.**  
  
**Objective: Explain the fundamental concepts and best practices related to authentication, authorization and access control**.  
  
Which of the following is another name for a CAC?

a) Token  
b) RFID  
c) MAC  
**d) PIV**

**Question 6.**  
  
**Objective: Explain the fundamental concepts and best practices related to authentication, authorization and access control**.  
  
Which of the following systems offers Trusted OS capabilities by default?

a) Windows Vista  
b) Windows 7  
**c) SE Linux**  
d) Backtrack

**Question 7.**  
  
**Objective: Carry out appropriate procedures to establish host security**.  
  
Which of the following describes a common operational problem when using patch management software that results in a false sense of security?

a) Conflicts with vulnerability scans impede patch effectiveness  
**b) Distributed updates may fail to apply or may not be active until a reboot**  
c) Vendor patches are released too frequently consuming excessive network bandwidth  
d) It is resource intensive to test all patches

**Question 8.**  
  
**Objective: Analyze and differentiate among types of attacks**.  
  
Which of the following is BEST identified as an attacker who has or is about to use a Logic bomb?

a) Grey hat  
**b) Malicious insider**  
c) White hat  
d) Black box

**Question 9.**  
  
**Objective: Explain the importance of security related awareness and training**.  
  
Which of the following is the BEST choice in regards to training staff members on dealing with PII?

a) PII requires public access but must be flagged as confidential  
b) PII data breaches are always the result of negligent staff and punishable by law  
**c) PII must be handled properly in order to minimize security breaches and mishandling**  
d) PII must be stored in an encrypted fashion and only printed on shared printers

**Question 10.**  
  
**Objective: Explain the importance of data security**.  
  
Which of the following processes are used to avoid employee exhaustion and implement a system of checks and balances?

**a) Job rotation**  
b) Incident response  
c) Least privilege  
d) On-going security

**Question 11.**  
  
**Objective: Explain risk related concepts**.  
  
When designing secure LDAP compliant applications, null passwords should NOT be allowed because:

a) null password can be changed by all users on a network  
**b) a null password is a successful anonymous bind**  
c) null passwords can only be changed by the administrator  
d) LDAP passwords are one-way encrypted

**Question 12.**  
  
**Objective: Explain the fundamental concepts and best practices related to authentication, authorization and access control**.  
  
A security administrator visits a remote data center dressed as a delivery person. Which of the following is MOST likely being conducted?

**a) Social engineering**  
b) Remote access  
c) Vulnerability scan  
d) Trojan horse

**Question 13.**  
  
**Objective: Analyze and differentiate among types of social engineering attacks**.  
  
Mobile devices used in the enterprise should be administered using:

a) encrypted networks and system logging  
b) full disk encryption and central password management  
c) vendor provided software update systems  
**d) centrally managed update services and access controls**

**Question 14.**  
  
**Objective: Implement appropriate security controls when performing account management**.  
  
The Chief Information Officer (CIO) wants to implement widespread network and hardware changes within the organization. The CIO has adopted an aggressive deployment schedule and does not want to bother with documentation, because it will slow down the deployment. Which of the following are the risks associated with not documenting the changes?

**a) Undocumented networks might not be protected and can be used to support insider attacks**  
b) Documenting a network hinders production because it is time consuming and ties up critical resources  
c) Documented networks provide a visual representation of the network for an attacker to exploit  
d) Undocumented networks ensure the confidentiality and secrecy of the network topology

**Question 15.**  
  
**Objective: Carry out appropriate risk mitigation strategies**.  
  
Which of the following could mitigate shoulder surfing?

**a) Privacy screens**  
b) Hashing  
c) Man traps  
d) Screen locks

**Question 16.**  
  
**Objective: Analyze and differentiate among types of mitigation and deterrent techniques** .  
  
Which of the following passwords is the MOST complex?

**a) 5@rAru99**  
b) CarL8241g  
c) j1l!1b5  
d) l@ur0

**Question 17.**  
  
**Objective: Implement appropriate security controls when performing account management**.  
  
Which of the following is being utilized when the BIOS and operating system’s responsibility is platform integrity?

a) SSL  
b) USB encryption  
c) Data loss prevention  
**d) TPM**

**Question 18.**  
  
**Objective: Explain the importance of data security**.  
  
Which of the following BEST describes a Buffer Overflow attack that allows access to a remote system?

a) The attacker attempts to have the receiving server run a payload using programming commonly found on web servers  
b) The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage  
c) The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information  
**d) The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload**

**Question 19.**  
  
**Objective: Analyze and differentiate among types of application attacks.**

A company fails to monitor and maintain the HVAC system in the datacenter. Which of the following is the MOST likely to affect availability of systems?

a) Employee productivity in a hot datacenter  
**b) Premature failure of components**  
c) Decreased number of systems in the datacenter  
d) Increased utility costs

**Question 20.**  
  
**Objective: Explain the impact and proper use of environmental controls.**

Which of the following protocols is defined in RFC 1157 as utilizing UDP ports 161 and 162?

**a) SNMP**  
b) IPSec  
c) SSL  
d) TLS

**Question 21.**  
  
**Objective: Explain the impact and proper use of environmental controls**.  
  
Which of the following is LEAST likely to have a legitimate business purpose?

a) Metasploit  
b) Vulnerability scanner  
**c) Steganography**  
d) Port scanner

**Question 22.**  
  
**Objective: Explain the importance of data security.**

Which of the following does full disk encryption on a laptop computer NOT protect against?

a) Confidentiality of the data  
**b) Key loggers**  
c) Theft of the data  
d) Disclosure of the data

**Question 23.**  
  
**Objective: Implement appropriate security controls when performing account management.**

Which of the following passwords exemplifies the STRONGEST complexity?

a) Passw0rd  
**b) P@ssw0rd**  
c) Passwrd  
d) passwordpassword

**Question 24.**  
  
**Objective: Implement assessment tools and techniques to discover security threats and vulnerabilities.**

Which following port ranges would give a technician the MOST comprehensive port scan of a server?

a) 1024-15000  
b) 0-99999  
**c) 0-65535**  
d) 0-1024

**Question 25.**  
  
**Objective: Analyze and differentiate among types of wireless attacks.**

Which of the following attacks steals contacts from a mobile device?

**a) Bluesnarfing**  
b) Smurf attack  
c) Session hijacking  
d) Bluejacking

**Question 26.**  
  
**Objective: Analyze and differentiate among types of wireless attacks.**

Which of the following attacks sends unwanted messages to a mobile device?

a) Session hijacking  
b) Smurf attack  
**c) Bluejacking**  
d) Bluesnarfing

**Question 27.**  
  
**Objective: Analyze and differentiate among types of attacks.**

A smurf attack relies on which protocol to perform a Denial of Service?

a) DNS  
b) SNMP  
c) SMTP  
**d) ICMP**

**Question 28.**  
  
**Objective: Distinguish and differentiate network design elements and components.**

Which of the following allows for multiple operating systems to run on a single piece of hardware?

**a) Virtualization**  
b) Port security  
c) Remote access  
d) DMZ

**Question 29.**  
  
**Objective: Explain the fundamental concepts and best practices related to authentication, authorization and access control.**

A user name is an example of which of the following?

**a) Identification**  
b) Authentication  
c) Authorization  
d) Access

**Question 30.**  
  
**Objective:** **Explain the core concepts of public key infrastructure.**

The CRL contains a list of:

a) private keys  
**b) public keys**  
c) root certificates  
d) valid certificates