Exam Report: 8.3.5 Practice Questions

Date: 6/17/2019 11:36:39 am
Time Spent: 0:56

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following information is typically **not** included in an access token?

- User security identifier
- User rights
- User account password
- Group membership

Explanation

The access token does not contain the user account password. The password is only used during authentication. Following authentication, the access token is used to gain access to resources.

When a security principal logs in, an access token is generated. The access token is used to control access to resources and contains the following information:

- The SID for the user or computer
- The SID for all groups the user or computer is a member of
- User rights granted to the security principal

When the security principal tries to access a resource or take an action, information in the access token is checked. For example, when a user tries to access a file, the access token is checked for the SID of the user and all groups. The SIDs are then compared to the SIDs in the object's DACL to identify permissions that apply.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_01]

Question 2: Correct

Which of the following terms describes the component that is generated following authentication and is used to gain access to resources following login?

- Access token
- Account policy
- Proxy
- Cookie

Explanation

When a security principal logs on, an access token is generated. The access token is used to control access to resources and contains the following information:

- The SID for the user or computer
- The SID for all groups the user or computer is a member of
- User rights granted to the security principal

When the security principal tries to access a resource or take an action, information in the access token is checked. For example, when a user tries to access a file, the access token is checked for the SID of the user and all groups. The SIDs are then compared to the SIDs in the object's DACL to identify permissions that apply.

Account policies in Group Policy control requirements for passwords, such as minimum length and expiration times. *Cookies* are text files that are stored on a computer to save information about your preferences, browser settings, and Web page preferences. They identify you (or your browser) to websites. A *proxy* is a server that stands between a client and destination servers.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_03]

Question 3: Correct

Marcus White has just been promoted to a manager. To give him access to the files that he needs, you make his user account a member of the Managers group, which has access to a special shared folder.

Later that afternoon, Marcus tells you that he is still unable to access the files reserved for the Managers group. What should you do?

- ○ Add his user account to the ACL for the shared folder
- ○ Manually refresh Group Policy settings on his computer
- ○ Manually refresh Group Policy settings on the file server
- ➡ ◉ Have Marcus log off and log back in

Explanation

On a Microsoft system, the access token is only generated during authentication. Changes made to group memberships or user rights do not take effect until the user logs in again and a new access token is created.

Use NTFS and share permissions, not Group Policy, to control access to files. In addition, Group Policy is periodically refreshed, with new settings applied on a regular basis.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_02]

Question 4: Correct

Which security mechanism uses a unique list that meets the following specifications:

- The list is embedded directly in the object itself
- The list defines which subjects have access to certain objects
- The list specifies the level or type of access allowed to certain objects

- ○ Mandatory access control
- ➡ ◉ User ACL

- Hashing
- Kerberos

Explanation

A user ACL (access control list) is a security mechanism that defines which subjects have access to certain objects and the level or type of access allowed. This security mechanism is unique for each object and embedded directly in the object itself.

Mandatory access control (MAC) is an access control system based on classifications of subjects and objects to define and control access. Kerberos is a form of single sign-on that uses hashed passwords to verify a user's identity. Hashing is a cryptographic tool that creates an identification code that is employed to detect changes in data.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_04]

Question 5: Correct

Lori Redford, who has been a member of the Project Management group, was recently promoted to manager of the team. She has been added as a member of the Managers group.

Several days after being promoted, Lori needs to have performance reviews with the team she manages but she cannot access the performance management system. As a member of the Managers group, she should have the Allow permission to access this system.

What is most likely preventing her from accessing this system?

- She is still a member of the Project Management group, which has been denied permission to this system. However, being a member of the Managers group should allow her to access this system. Allow permissions always override Deny permissions. There must be an explicit permission entry that is preventing her from accessing the management system.
- ➡ She is still a member of the Project Management group, which has been denied permission to this system. Deny permissions always override Allow permissions.
- Her user object has been assigned an explicit Deny permission to the performance management system.
- Her user object has been assigned an explicit Allow permission to the performance management system, but she inherits the Deny permission assigned to the Project Management group (which she still belongs to). Inherited Deny permissions override explicit Allow permissions.

Explanation

The most likely cause of this problem is that Lori is still a member of the Project Management group which has been denied permission to this system. Deny permissions always override Allow permissions.

Allow permissions do not override Deny permissions, unless the Allow permission is explicitly assigned and the Deny permission is inherited. It is unlikely that her user object has been assigned an explicit Deny permission to the performance management system since best practice is to assign permissions to groups, not to users.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_05]

Exam Report: 8.4.9 Practice Questions

Date: 6/17/2019 6:32:14 pm
Time Spent: 1:54

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You want to prevent your browser from running JavaScript commands that are potentially harmful. Which of the following would you restrict to accomplish this?

- ActiveX
- CGI
- Server-side scripts
- Client-side scripts

Explanation

JavaScript is an example of client-side scripting, where the client system runs the scripts that are embedded in Web pages. When pages download, the scripts are executed.

ActiveX runs executable code within a browser, but ActiveX controls are not written using the JavaScript language. Server-side scripts execute on the server, and modify the Web pages served to clients based on the results of the scripts. The Common Gateway Interface (CGI) is scripting language that is often used to capture data from forms in a Web page and pass the data to an external program. CGI runs on the server to process Web form data.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_01]

Question 2: Correct

A programmer that fails to check the length of input before processing leaves his code vulnerable to what form of common attack?

- Buffer overflow
- Backdoor
- Session hijacking
- Privilege escalation

Explanation

Buffer overflow attacks are made possible by oversight of programmers. A simple check on the length (and sometimes format) of input data before processing eliminates buffer attacks.

A *backdoor* is a developer-planted or cracker-planted entry device that bypasses security to gain

access to a system or software. A developer-planted backdoor is often a debugging tool that was mistakenly left in place when the software went to market. A cracker-planted device is often a remote access server that listens for inbound connections on a specific port. Either method can be used by an intruder to gain entry into a secured environment.
Session hijacking is the concept of being able to take over a communication session between a client and server. This usually involves taking over the identity of the client and fooling the server into communicating with the pseudo client. Privilege escalation is the act of a user to steal or obtain higher level privileges in a computer system.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_03]

Question 3: Correct

Which of the following is an attack that injects malicious scripts into Web pages to redirect users to fake websites or gather personal information?

- ○ Drive-by download
- ○ DLL injection
- ○ SQL injection
- ➡ ◉ XSS

Explanation

Cross-site scripting (XSS) is an attack that injects scripts into Web pages. When the user views the Web page, the malicious scripts run allowing the attacker to capture information or perform other actions.

- XSS often relies on social engineering or phishing to entice users to click on links to Web pages that contain the malicious scripts.
- Some scripts redirect users to legitimate websites, but run the script in the background to capture information sent to the legitimate site.
- Scripts can be written to read (steal) cookies that contain identity information (such as session information).
- Scripts can also be designed to run under the security context of the current user. For example, scripts might execute with full privileges on the local system, or the scripts might run using the credentials used on a financial website.

A drive-by download is an attack where software or malware is downloaded and installed without explicit consent from the user. A *SQL injection* attack occurs when an attacker includes database commands within user data input fields on a form, and those commands subsequently execute on the server. A *DLL injection* attack occurs when a program is forced to load a dynamic-link library (DLL). This DLL then executes under the security context of the running application, and executes malicious code included with the injected DLL.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_04]

Question 4: Correct

When you browse to a website, a pop-up window tells you that your computer has been infected with a virus. You click on the window to see what the problem is. Later, you find out that the window has installed spyware on your system.

What type of attack has occurred?

- ○ Trojan horse
- ➡ ◉

Drive-by download

SQL injection

DLL injection

Explanation

A drive-by download is an attack where software or malware is downloaded and installed without explicit consent from the user. Drive-by downloads can occur in a few different ways:

- Through social engineering, the user is tricked into downloading the software. The user might not realize that clicking a link will install software, or the user might know that something is being installed, but not have a full understanding of what it is or what it does.
- By exploiting a browser or operating system bug, a site is able to install software without the user's knowledge or consent.

A *SQL injection* attack occurs when an attacker includes database commands within user data input fields on a form, and those commands subsequently execute on the server. A *DLL injection* attack occurs when a program is forced to load a dynamic-link library (DLL). This DLL then executes under the security context of the running application, and executes malicious code included with the injected DLL. A Trojan horse is a program that masquerades as a legitimate program. In this scenario, you were not necessarily aware that a program was being installed, nor did the program present itself as a useful program for you to install.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_05]

Question 5: Correct

Which of the following are subject to SQL injection attacks?

Database servers

Browsers that allow client-side scripts

Web servers serving static content

ActiveX controls

Explanation

A *SQL injection* attack occurs when an attacker includes database commands within user data input fields on a form, and those commands subsequently execute on the server. The injection attack succeeds if the server does not properly validate the input to restrict entry of characters that could end and begin a database command.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_06]

Question 6: Correct

You have a website that accepts input from users for creating customer accounts. Input on the form is passed to a database server where the user account information is stored.

An attacker is able to insert database commands in the input fields and have those commands execute on the server.

Which type of attack has occurred?

DLL injection

Cross-site scripting

- SQL injection
- Buffer overflow

Explanation

A *SQL injection* attack occurs when an attacker includes database commands within user data input fields on a form, and those commands subsequently execute on the server. The injection attack succeeds if the server does not properly validate the input to restrict entry of characters that could end and begin a database command. SQL injection attacks are prevented by proper programming methods that prevent commands from occurring within form data or that filter data to prevent such attacks.

A *buffer overflow* occurs when the operating system or an application does not properly enforce boundaries for how much and what type of data can be inputted. Hackers submit data beyond the size reserved for the data in the memory buffer, and the extra data overwrites adjacent memory locations. The extra data sent by the attacker could include executable code that might then be able to execute in privileged mode.

Cross-site scripting (XSS) is an attack that injects scripts into Web pages. When the user views the Web page, the malicious scripts run allowing the attacker to capture information or perform other actions. A *DLL injection* attack occurs when a program is forced to load a dynamic-link library (DLL). This DLL then executes under the security context of the running application, and executes malicious code included with the injected DLL.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_07]

Question 7: Correct

Having poor software development practices and failing to program input validation checks during development of custom software can result in a system vulnerable to which type of attack?

- Superzapping
- Dictionary
- Buffer overflow
- Denial of service

Explanation

Poor software development practices and failing to program input validation checks can leave a system vulnerable to buffer overflows. A buffer overflow occurs when software code receives more input than it was designed to handle and the programmer of that code failed to include input validation checks. When a buffer overflow occurs, the extra data is pushed into the execution stack and processed with the security context of the system itself. In other words, a buffer overflow attack often allows the attacker to perform any operation on a system.

Denial of service attacks exploit vulnerabilities in implementation and coding errors. Dictionary attacks are waged against logon prompts or stolen copies of a security accounts database. Superzapping attacks are specific attacks using a specialized utility named superzap to bypass the security of IBM mainframes to perform system alterations.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_10]

Question 8: Correct

Which type of attack is the act of exploiting a software program's free acceptance of input in

order to execute arbitrary code on a target?

- TOC/TOU
- Buffer overflow
- Covert channel exploitation
- Data diddling

Explanation

The act of exploiting a software program's free acceptance of input in order to execute arbitrary code on a target is called a buffer overflow.

Data diddling is the changing or corrupting of data. TOC/TOU is a logon session replay attack. Covert channel exploitation is the use of timing or storage mechanisms to bypass security controls in order to leak information out of a secured environment.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_11]

Question 9: Correct

As you browse the Internet, you notice that when you go to some sites, multiple additional windows are opened automatically. Many of these windows contain advertisements for products that are inappropriate for your family to view.

Which tool can you implement to prevent these windows from showing?

- Anti-virus
- Anti-spyware
- Anti-adware
- Pop-up blocker
- Phishing filter

Explanation

Use a pop-up blocker to prevent windows from automatically opening when you visit a Web site. Pop-up blockers typically do not block pop-ups that show when you click a button or a link, but will prevent the pop-up windows that open automatically as you navigate to other sites.

Use anti-virus software to scan attachments, downloads, or your system for malicious programs. Use anti-adware and anti-spyware software to prevent software that tracks your browsing history. While removing adware might prevent some pop-ups, it will not prevent all pop-ups unless the anti-adware software includes a pop-up blocker. Use a phishing filter to remove phishing e-mails or to prevent navigating to links that are disguised as legitimate links.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_12]

Question 10: Correct

While using a Web-based order form, an attacker enters an unusually large value in the Quantity field.

The value she entered is so large that it exceeds the maximum value supported by the variable type used to store the quantity in the Web application. This causes the value of the quantity

variable to wrap around to the minimum possible value, which is a negative number.

As a result, the Web application processes the order as a return instead of a purchase, and the attacker's account is refunded a large sum of money.

What type of attack has occurred in this scenario?

- (selected) Integer overflow
- Buffer overflow
- URL hijacking
- Watering hole

Explanation

An *integer overflow* occurs when a computational operation by a running process results in a numeric value that exceeds the maximum size of the integer type used to store it in memory. When this occurs, the value will wrap around and start again at its minimum value, in much the same way a mechanical odometer in a car rolls over to zero when the maximum number of miles it can record has been exceeded. This can allow an attacker to manipulate the value of variables, leading to unintended behavior by the system. In this scenario, the attacker has manipulated the quantity while purchasing items from an online store. This causes the value of the quantity variable to wrap around to the minimum possible value, which is a negative number. As a result, the web application processes the order form as a return instead of a purchase and the attacker's account is refunded a large sum of money.

A *buffer overflow* occurs when the operating system or an application does not properly enforce boundaries for how much and what type of data can be inputted. In a *watering hole* attack, the attacker uses reconnaissance to identify which Web sites the target person or organization frequently uses. The attacker then compromises one or more of those sites in some way, hoping that the target will access the site and be exposed to the exploit. *URL hijacking* occurs when an attacker registers domain names that correlate to common typographical errors made by users when trying to access a legitimate Web site.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_13]

Question 11: Correct

While using a Web-based game created using Adobe Flash, a Flash cookie is set on a user's computer. The game saves legitimate data in the Flash cookie, such as statistics and user preferences.

However, the game creator also programmed the game to track the Web sites that that user visits while the game is running and save them in the Flash cookie. This data is transferred to a server over an Internet connection without the user's permission.

What type of exploit has occurred in this scenario?

- Zero-day
- Buffer overflow
- (selected) Locally shared object (LSO) exploit
- Header manipulation

Explanation

A *locally shared object* (LSO) exploit has occurred in this scenario. LSOs are also referred to as *Flash cookies*. Adobe Flash uses LSOs to save data locally on a computer, such as information for a Flash game being played or user preferences. However, LSOs can also be used to collect

information about the user's browsing habits without their permission. The Flash Player Settings Manager can be used to configure Flash to prevent LSOs from being saved on the local computer.

A *buffer overflow* occurs when the operating system or an application does not properly enforce boundaries for how much and what type of data can be inputted. *Header manipulation* is the process of including invalid data in an HTTP response header. A *zero-day* attack is an attack that exploits computer application vulnerabilities before they are known and patched by the application's developer.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_14]

Question 12: Correct

Recently, a Web site named www.vidshare.com has become extremely popular with users around the world. An attacker registers the following domain names:

- www.videoshare.com
- www.vidshar.com
- www.vidsshare.com

Each of these URLs points to a phishing Web site that tricks users into supplying their vidshare.com user names and passwords.

What type of attack has occurred in this scenario?

- Buffer overflow
- Watering hole
- Command injection
- Typosquatting

Explanation

Typosquatting (also called *URL hijacking*) occurs when an attacker registers domain names that correlate to common typographical errors made by users when trying to access a legitimate Web site. The typosquatter's intentions may be benign or malicious in nature. They may be simply trying to coerce the legitimate site owner to buy the domain name from them. Alternatively, they may be attempting to compromise unsuspecting users by redirecting them to a phishing site that looks like the legitimate Web site. They may even use this exploit to install drive-by malware.

A *buffer overflow* occurs when the operating system or an application does not properly enforce boundaries for how much and what type of data can be inputted. In a *watering hole* attack, the attacker uses reconnaissance to identify which Web sites the target person or organization frequently uses. The attacker then compromises one or more of those sites in some way, hoping that the target will access the site and be exposed to the exploit. In a *command injection* attack, the attacker injects and executes unwanted commands on the application.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_15]

Question 13: Correct

Match the exploit on the right with the appropriate description on the left.

Watering hole attack

- An attacker compromises a Web site, hoping that a target individual will access the site and

be exposed to the exploit.

Arbitrary code execution exploit

- ✔ A vulnerability in a running process allows an attacker to inject malicious instructions and run them.

LSO exploit

- ✔ A Flash cookie is used to collect information about the user's browsing habits without their permission.

Zero-day attack

- ✔ An attacker exploits computer application vulnerabilities before they are known and patched by the application's developer.

Explanation

In *a watering hole* exploit, an attacker compromises a Web site, hoping that a target individual will access the site and be exposed to the exploit. In an *arbitrary code execution* exploit, a vulnerability in a running process allows an attacker to inject malicious code and run it. In a *zero-day* exploit, an attacker exploits computer application vulnerabilities before they are known and patched by the application's developer. In a *locally-shared object* (LSO) exploit, a Flash cookie is used to collect information about the user's browsing habits without their permission.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_16]

Question 14: Correct

An attacker inserts SQL database commands into a data input field of an order form used by a Web-based application. When submitted, these commands are executed on the remote database server, causing customer contact information from the database to be sent to the malicious user's Web browser.

Which practice would have prevented this exploit?

- ○ Implementing a script blocker.
- ○ Installing antivirus, anti-spyware, pop-up blockers, and firewall software.
- ➡ ◉ Implementing client-side validation.
- ○ Using the latest browser version and patch level.

Explanation

Client-side validation should have been used on the local system to identify input errors in the order form before the data was ever sent to the server. In this example, if the user entered SQL commands in an order form field, the error would have been immediately detected and blocked before the data was submitted to the server.

Using the latest browser version and patch level, installing anti-malware software, and using a script blocker are valuable security measures, but would not have prevented the exploit in this scenario.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_17]

Question 15: Correct

While using a Web-based order form, an attacker enters an unusually large value in the Quantity field.

The value she entered is so large that it exceeds the maximum value supported by the variable

type used to store the quantity in the Web application. This causes the value of the quantity variable to wrap around to the minimum possible value, which is a negative number.

As a result, the Web application processes the order as a return instead of a purchase, and the attacker's account is credited with a large sum of money.

Which practices would have prevented this exploit? (Select two.)

- [ ] Installing antivirus, anti-spyware, pop-up blockers, and firewall software.
- [x] Implementing server-side validation.
- [ ] Installing the latest operating system updates.
- [ ] Using the latest browser version and patch level.
- [x] Implementing client-side validation.

Explanation

Client-side validation and *server-side validation* should have been used to identify input errors in the order form. In this example, if the user entered an invalid quantity in an order form field, client-side validation would have detected and blocked the error before the data was submitted to the server. Server-side validation should have also been used after the data was sent to the server to detect errors. Experienced attackers can circumvent client-side validation techniques by sending data to the server from outside the application's standard user interface, bypassing any input validation measures that may have been implemented on the client.

Using the latest browser version and patch level, installing the latest operating system updates, and using a script blocker are valuable security measures, but would not have prevented the exploit in this scenario.

References

LabSim for Security Pro, Section 8.4.
[All Questions SecPro2017_v6.exm WEB_APP_ATTACKS_18]

Exam Report: 8.5.10 Practice Questions

Date: 6/18/2019 6:25:10 pm
Time Spent: 0:51

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Use of which of the following is a possible violation of privacy?

- VPNs
- ➡ Cookies
- HTTP
- FTP

Explanation

Use of cookies is a possible violation of privacy. Cookies can be used to record information about your computer system, your web surfing habits, and much more. Secured environments should restrict the use of cookies on all web browsers and other internet service utilities.

The use of Java, VPNs, and FTP do not usually represent privacy violations.

References

LabSim for Security Pro, Section 8.5.
[All Questions SecPro2017_v6.exm INTERNET_BROWSERS_01]

Question 2: Correct

Which of the following is **not** true regarding cookies?

- They can retain connection and session information
- They can help a hacker spoof a user's identity
- ➡ They operate within a security sandbox
- They can collect user information

Explanation

Cookies do not operate within a security sandbox. The concept of a security sandbox is related to Java. Cookies have as much access to a system as the user account under which they were brought on to the system. Use of cookies is a possible violation of privacy. Cookies can be used to record information about your computer system, your web surfing habits, and much more. Secured environments should restrict the use of cookies on all web browsers and other internet service utilities.

References

LabSim for Security Pro, Section 8.5.

[All Questions SecPro2017_v6.exm INTERNET_BROWSERS_02]

Question 3: Correct

Which of the following is a text file provided by a website to a client that is stored on a user's hard drive in order to track and record information about the user?

- Digital signature
- Mobile code
- Certificate
- Cookie

Explanation

A *cookie* is text file that a website provides to a client that is stored on a user's hard drive in order to track and record information about the user.

Mobile code is self-contained software that is transferred to a web client to be executed. It allows for client-side execution of web applications. A *certificate* is a digital proof of identity used to establish or verify who someone is over a network or the internet. A *digital signature* is a cryptographic tool that is used to prove who a message is from and that the contents of the message did not change or become altered while in transit.

References

LabSim for Security Pro, Section 8.5.
[All Questions SecPro2017_v6.exm INTERNET_BROWSERS_03]

Question 4: Correct

You want to allow e-commerce websites that you visit to keep track of your browsing history for shopping carts and other information, but want to prevent that information from being tracked by sites linked to the sites you explicitly visit.

How should you configure the browser settings?

- Prevent ActiveX controls and Java on linked websites
- Allow first party cookies, but block third-party cookies
- Enable the phishing filter to check all embedded links in webpages you visit
- Block cross-site scripting (XSS)

Explanation

Cookies are text files that are stored on a computer to save information about your preferences, browser settings, and webpage preferences. *First party* cookies are cookies used by the site you are visiting; *third party* cookies are cookies placed by sites linked to the site you are visiting. For example, banner ads on a website might place cookies on your machine to identify ads you have already seen or ads you have clicked on.

ActiveX and Java are executable programs that run in the browser. While they could be written to track user history, they would typically use cookies for storing that information.

Cross-site scripting (XSS) is an attack that injects scripts into webpages. When the user views the webpage, the malicious scripts run, allowing the attacker to capture information or perform other actions. Phishing uses links that appear legitimate, but are directed to false websites for the purpose of installing malware or gathering information from users.

References

LabSim for Security Pro, Section 8.5.
[All Questions SecPro2017_v6.exm INTERNET_BROWSERS_04]

Question 5: Correct

What is a *cookie*?

- A malicious program that runs when you read an email attachment.
- A malicious program that disguises itself as a useful program.
- An executable file that runs in the background and tracks internet use.
- A file saved on your hard drive that tracks website preferences and use.

Explanation

A *cookie* is a file saved on your hard drive that tracks website preferences and use. Many legitimate websites use cookies to remember your preferences and make the websites easier to use. However, other sites can use cookies to track personal information.

Spyware is a program that runs in the background and reports internet use to servers on the internet. A Trojan horse is a malicious program that disguises itself as a useful program. Programs do not run when you simply read an email attachment. However, many malicious script programs are disguised as simple text files and can cause damage if you run the script file.

References

LabSim for Security Pro, Section 8.5.
[All Questions SecPro2017_v6.exm INTERNET_BROWSERS_05]

Question 6: Correct

To help prevent browser attacks, users of public computers should do which of the following?

- Turn the public computer off immediately after use
- Ensure that public login credentials are unique
- Clear the browser cache
- Not use any public computer that has been used in the last 30 minutes

Explanation

To provide some level of protection, you should clear the browser cache whenever you use a public computer to access the internet, especially when you have accessed sites for retrieving personal data.

Typically, users of public computers are not given unique login credentials. Using a computer that has been used in the last 30 minutes does not prevent or induce browser attacks. Turning off a computer immediately after use does prevent another person from using it for a short time but does not prevent browser attacks, as sensitive information is still found in the browser cache.

References

LabSim for Security Pro, Section 8.5.
[All Questions SecPro2017_v6.exm INTERNET_BROWSERS_06]

Question 7: Correct

You manage several Windows systems.

Desktop users access an in-house application that is hosted on your intranet web server. When a user clicks a specific option in the application, they receive an error message that the pop-up was blocked. You need to configure the security settings so that users can see the pop-up without compromising overall security.

What should you do?

- In Internet Options, use the Privacy tab to turn off Pop-up Blocker.
- Add the URL of the website to the Local intranet zone.
- Change the filter level in Pop-up Blocker to High.
- Change the filter level in Pop-up Blocker to Medium.

Explanation

Add the URL of the intranet website to the Local intranet zone. This gives the website a higher security clearance. By default, the Local intranet zone turns Pop-up Blocker off, allowing pop-ups from all sites in the zone.

When you change the filter level in Pop-up Blocker to Medium or High, it still blocks pop-ups. If you disable the Pop-up Blocker, all pop-ups are displayed.

References

LabSim for Security Pro, Section 8.5.
[All Questions SecPro2017_v6.exm INTERNET_BROWSERS_07]

Question 8: Correct

You manage several Windows systems. All computers are members of a domain.

You use an internal website that uses Integrated Windows Authentication. You attempt to connect to the website and are prompted for authentication.

You verify that your user account has permission to access the website. You need to ensure that you are automatically authenticated when you connect to the website.

What should you do?

- Add the internal website to the Trusted sites zone.
- Add the internal website to the Local intranet zone.
- Create a complex password for your user account.
- Open Credential Manager and modify your credentials.

Explanation

You must add the internal website to the Local intranet zone. By default, only Local intranet zones allow Integrated Windows Authentication. With Integrated Windows Authentication, the user name and password are hashed before being sent across the network.

The Trusted Sites zone often requires elevated privileges. By default, the sites that are added to the Trusted Sites zone must be in the form of https:// or secured with a Secure Sockets Layer (SSL) certificate. Credential Manager stores account credentials for network resources, such as file servers and websites. Password complexity prevents passwords that are easy to guess or easy to crack.

References

LabSim for Security Pro, Section 8.5.
[All Questions SecPro2017_v6.exm INTERNET_BROWSERS_08]

Exam Report: 8.6.12 Practice Questions

Date: 6/19/2019 12:34:57 pm
Time Spent: 0:36

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following enters random data to the inputs of an application?

- Validation rules
- Application hardening
- Fuzzing
- Routines

Explanation

Fuzz testing (also known as *fuzzing*) is a software testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application. Fuzzing programs come in two types:

- *Mutation-based* programs, which mutate existing data samples to create test data.
- *Generation-based* programs, which define new test data based on models of the input.

Input validation is the process of ensuring that a program operates on clean, correct, and useful data. Input validation uses *routines* (also called *validation rules* or *check routines*) that check for correctness, meaningfulness, and secureness in data input to the system. Application hardening is the process of preventing vulnerability exploitation in software applications.

References

LabSim for Security Pro, Section 8.6.
[All Questions SecPro2017_v6.exm APP_DEV_01]

Question 2: Correct

Which of the following is specifically meant to ensure that a program operates on clean, correct, and useful data?

- Error and exception handling
- Process spawning
- Input validation
- Application hardening

Explanation

Input validation is the process of ensuring that a program operates on clean, correct, and useful data. Input validation uses *routines* (also called *validation rules* or *check routines*) that

check for correctness, meaningfulness, and secureness in data input to the system.

Application hardening is the process of preventing vulnerability exploitation in software applications. Error and exception handling is a programming language construct designed to handle the occurrence of exceptions (which are special conditions that change the normal flow of program execution). Process spawning is the creation of a new process (also called a child process) by an existing process (also called a parent process).

References

LabSim for Security Pro, Section 8.6.
[All Questions SecPro2017_v6.exm APP_DEV_02]

Question 3: Correct

During the application development cycle, an application tester creates multiple virtual machines on a hypervisor, each with a different version and edition of Windows installed. She then installs the latest build of the application being developed on each virtual machine and evaluates each installation for security vulnerabilities.

Which assessment technique was used in this scenario?

- (selected) Configuration testing
- Code review
- Baseline reporting
- Fuzzing

Explanation

Configuration testing is the process of testing an application under development on systems that have various combinations of hardware and software. In this scenario, the tester is evaluating the security of the application on various versions and editions of the Windows operating system.

A code review is systematic examination of an application's source code. It is intended to find and fix overlooked mistakes, improving the overall quality and security of software. A code review is sometimes called a *peer review*. Fuzzing is a software testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application. Input validation is the process of ensuring that a program operates on clean, correct, and useful data.

References

LabSim for Security Pro, Section 8.6.
[All Questions SecPro2017_v6.exm APP_DEV_03]

Question 4: Correct

During the application development cycle, a developer asks several of his peers to assess the portion of the application he was assigned to write for security vulnerabilities.

Which assessment technique was used in this scenario?

- Baseline reporting
- Fuzzing
- Input validation
- (selected) Code review

Explanation

A code review is a systematic examination of an application's source code. It is intended to find

and fix overlooked mistakes, improving the overall quality and security of software. A code review is sometimes called a *peer review*.

Baselines are of a set of consistent requirements that establish a standard configuration for all systems. With a baseline established, you can more easily identify abnormal activity and areas that need improvement. Fuzzing is a software testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application. Input validation is the process of ensuring that a program operates on clean, correct, and useful data.

References

LabSim for Security Pro, Section 8.6.
[All Questions SecPro2017_v6.exm APP_DEV_04]

Question 5: Correct

You've been assigned to evaluate NoSQL databases as a part of a big data analysis initiative in your organization.

You've downloaded an open source NoSQL database from the internet and installed it on a test system in an isolated lab environment.

Which of the following are likely to be true about this test system? (Select two.)

- [ ] By default, data is stored in the database in an encrypted format.
- [ ] The database is more susceptible to SQL injection attacks than traditional SQL databases.
- [x] Data is stored in the database in an unencrypted format.
- [ ] The default admin user password is admin.
- [x] The database admin user has no password assigned.

Explanation

Because NoSQL is a relatively new database architecture and less mature than traditional SQL, there are several key security issues to be aware of:

• Most NoSQL database implementations do not require authentication by default, even for the admin user. After installation, user account passwords must be manually configured by the database administrator. Otherwise, anyone can access the database and view the information it contains without supplying a password.
• In most NoSQL database implementations, any logged in user can access every collection on the server by default. The database administrator must manually configure access controls to prevent unauthorized access to the information in the database.
• Most NoSQL database implementations do not implement data encryption for either data at rest or data in transit.
• Because NoSQL does not support most aspects of the SQL language, NoSQL databases are less susceptible to SQL injection attacks when compared to traditional SQL database implementations.

References

LabSim for Security Pro, Section 8.6.
[All Questions SecPro2017_v6.exm APP_DEV_05]

Question 6: Correct

You've been given an assignment to evaluate NoSQL databases as a part of a big data analysis initiative in your organization.

You've downloaded an open source NoSQL database from the internet and installed it on a test system in an isolated lab environment.

What should you do to harden this database before implementing it in a production environment? (Select two.)

- [ ] Implement an IDS to detect SQL injection attacks on the database
- [ ] Enable data encryption in the database configuration
- [x] Implement an application-layer protocol to encrypt data prior to saving it in the database
- [x] Disable anonymous access
- [ ] Enable anonymous access

Explanation

To harden a NoSQL implementation, consider using the following measures:

- Configure user accounts and assign strong passwords to them.
- Disable anonymous access and require authentication.
- Configure access controls to restrict access based on the user account.
- Encrypt data using an Application-layer protocol prior to saving it in the database. Databases don't like encryption, but this ensures that the data at rest is stored in an encrypted format within the database.
- Encrypt data in transit using SSL.
- Implement a NoSQL database only in in a hardened, secure environment protected by traditional network security mechanisms, such as firewalls, VLANs, and ACLs. NoSQL databases have limited security.

Because NoSQL does not support most aspects of the SQL language, NoSQL databases are less susceptible to SQL injection attacks when compared to traditional SQL database implementations.

References

LabSim for Security Pro, Section 8.6.
[All Questions SecPro2017_v6.exm APP_DEV_06]

Exam Report: 8.7.5 Practice Questions

Date: 6/19/2019 5:50:35 pm
Time Spent: 1:00

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following is an example of a decentralized privilege management solution?

- Active Directory
- RADIUS
- TACACS+
- Workgroup

Explanation

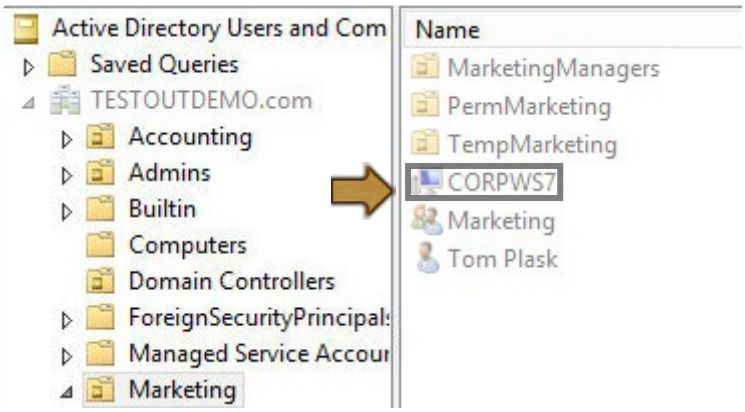
A workgroup is an example of a decentralized privilege management solution. In a workgroup, user accounts are defined on each individual system rather than on a centralized access control server. All of the other selections are centralized privilege management solutions.

References

LabSim for Security Pro, Section 8.7.
[All Questions SecPro2017_v6.exm ACT_DIR_OVW_01]

Question 2: Correct

Click on the object in the TESTOUTDEMO.com Active Directory domain that is used to manage individual desktop workstation access.



Explanation

Computer objects are used to manage access for individual computer systems in the domain, including servers, desktops, and notebooks. In this example, the desktop named CORPWS7 is represented by a corresponding computer object in the domain.

A *domain* (in this case TESTOUTDEMO.com) is an administratively defined collection of network

resources that share a common directory database and security policies. An *organizational unit* (OU) subdivides and organizes network resources within a domain. Several OUs are displayed in this scenario, including MarketingManagers, PermMarketing, and TempMarketing. *User objects* are used to manage access for individual employees. In this scenario, the employee named Tom Plask is represented by a corresponding user object in the domain.

References

LabSim for Security Pro, Section 8.7.
[All Questions SecPro2017_v6.exm ACT_DIR_OVW_03]

Question 3: Correct

Which of the following best describes Active Directory?

- A collection of related domain trees that establishes the relationship between trees that have different DNS namespaces
- A group of related domains that share the same contiguous DNS namespace
- An administratively-defined collection of network resources that share a common directory database and security policies
- A centralized database that contains user account and security information

Explanation

Active Directory is a centralized database that contains user account and security information. With Active Directory, all computers share the same central database.

Following are a few of the components of Active Directory:

- A domain is an administratively-defined collection of network resources that share a common directory database and security policies.
- A tree is a group of related domains that share the same contiguous DNS namespace.
- A forest is a collection of related domain trees. The forest establishes the relationship between trees that have different DNS namespaces.

References

LabSim for Security Pro, Section 8.7.
[All Questions SecPro2017_v6.exm ACT_DIR_OVW_04]

Question 4: Correct

Drag the Active Directory component on the left to the appropriate description on the right.

A server that holds a copy of the Active Directory database that can be written to.

Domain Controller

A folder that subdivides and organizes network resources within a domain.

Organizational Unit

An administratively-defined collection of network resources that share a common directory database and security policies.

Domain

A computing element that identifies resources in the Active Directory database.

Objects

Explanation

Active Directory organizes network resources and simplifies management using components that include the following:

Domains, which are administratively-defined collections of network resources that share a common directory database and security policies. A domain is the basic administrative unit of an Active Directory structure. Depending on the network structure and requirements, the entire network might be represented by a single domain with millions of objects, or the network might require multiple domains.

Active Directory also uses organizational units, which are like folders that subdivide and organize network resources within a domain. An organizational unit:

- Is a container object
- Can hold other organizational units
- Can hold objects such as users and computers
- Can be used to logically organize network resources
- Simplifies security administration

There are also objects within Active Directory. Each resource is identified as an object. Common objects include:

- Users
- Groups
- Computers
- Printers
- Shared folders

A domain controller is a server that holds a copy of the Active Directory database that can be written to. Replication is the process of copying changes to Active Directory between the domain controllers. In contrast, member servers are servers in the domain that do not have the Active Directory database.

References

LabSim for Security Pro, Section 8.7.
[All Questions SecPro2017_v6.exm ACT_DIR_OVW_05]

Question 5: Correct

Active Directory is a hierarchical database. Hierarchical directory databases have several advantages over flat file database structures.

Which of the following is **not** an advantage of Active Directory's hierarchical database structure?

- Scalability
- Delegation
- Organization
- Replication
- Decentralization

Explanation

Decentralization is **not** an advantage of Active Directory's hierarchical database structure. Active Directory makes it possible for all computers to share the same central database, which makes management much easier than when using a decentralized, flat database solution (such as a workgroup).

Hierarchical directory databases have the following advantages over flat file database structure:

- Organization
- Delegation

- Replication
- Scalability

References

LabSim for Security Pro, Section 8.7.
[All Questions SecPro2017_v6.exm ACT_DIR_OVW_06]

Exam Report: 8.8.9 Practice Questions

Date: 6/20/2019 10:44:43 am
Time Spent: 0:34

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What should you do to a user account if the user goes on an extended vacation?

- Remove all rights from the account
- Disable the account
- Monitor the account more closely
- Delete the account

Explanation

Disabling the account is the best measure to protect an inactive account. This prevents the account from being used for login.

If you delete the account or the rights assigned to the account, you will have to re-create the account or the rights when the user returns. Leaving the account active might expose it to attack, even if you regularly monitor it.

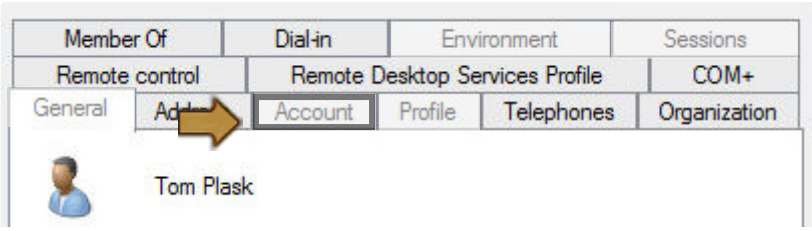
References

LabSim for Security Pro, Section 8.8.
[All Questions SecPro2017_v6.exm DOM_USRSGRPS_01]

Question 2: Correct

Tom Plask's user account has been locked because he entered too many incorrect passwords. You need to unlock the account.

Click the tab in the properties of the Tom Plask user object you would use to unlock his account.



Explanation

An account that has been locked out because too many incorrect passwords have been entered must be unlocked before the user will be allowed to authenticate. To unlock an account, go to the Account tab in the account object's Properties dialog, and then click Unlock Account.

The General tab allows you to enter information, such as the user's name, phone number, and

e-mail address. The Profile tab allows you to configure the path to the user's profile folder. The Environment tab allows you to configure the user's computing environment when he or she logs in. The Sessions tab allows you to configure session limits.

References

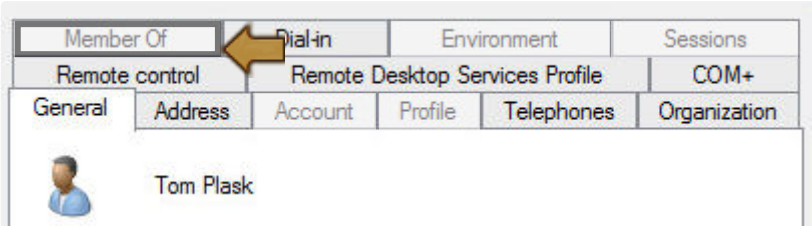
LabSim for Security Pro, Section 8.8.
[All Questions SecPro2017_v6.exm DOM_USRSGRPS_02]

Question 3: Correct

Tom Plask was recently transferred to the Technical Support department. He now needs access to the network resources used by Support employees.

To grant him access, you need to add Tom Plask's user account to the Support group in the Active Directory domain.

Click the tab in the properties of the Tom Plask user object you would use to accomplish this.



Explanation

The Member of tab in the properties of a user account allows an administrator to add or remove a user from an Active Directory group. Once a member of a group, the user is automatically granted access to the network resources that are granted to the group.

The Account tab is used to manage account related settings. The Profile tab allows you to configure the path to the user's profile folder. The Environment tab allows you to configure the user's computing environment when he or she logs in. The Sessions tab allows you to configure session limits.

References

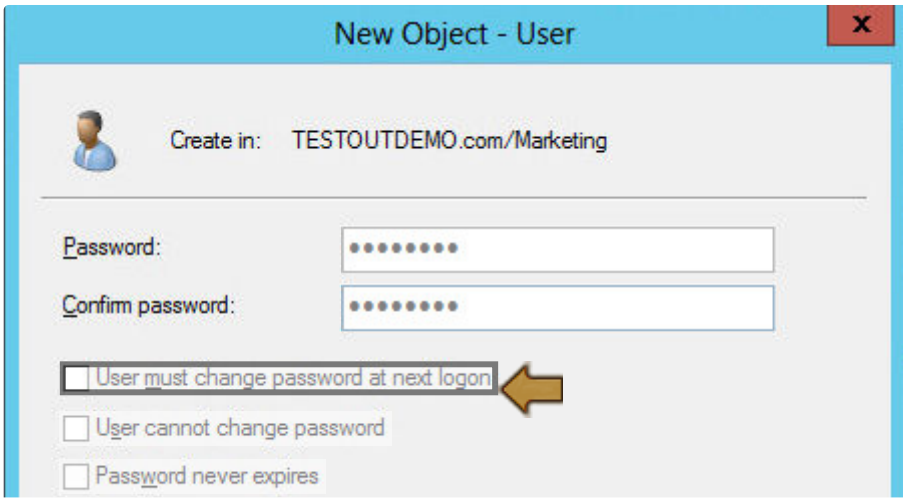
LabSim for Security Pro, Section 8.8.
[All Questions SecPro2017_v6.exm DOM_USRSGRPS_03]

Question 4: Correct

You are creating a new Active Directory domain user account for the Rachel McGaffey user account. During the account setup process, you assigned a password to the new account.

However, you know that the system administrator should not know any user's password for security reasons. Only the user should know his or her own password—no one else.

Click the option you would use in the New Object - User dialog to remedy this situation.



Explanation

When creating a new user account or resetting a forgotten password, a common practice is to reset the user account password and select User must change password at next logon. This forces the user to reset the password immediately following logon, ensuring the user is the only person who knows the password.

Enable the User cannot change password option when you want to maintain control over a guest, service, or temporary account. For example, many applications use service accounts for performing system tasks. The application must be configured with the user account name and password. In this situation, you may also need to enable the Password never expires option. The Account is disabled option is used in situations where you want to create an account now, but the user will not actually need it until a future date.

References

LabSim for Security Pro, Section 8.8.
[All Questions SecPro2017_v6.exm DOM_USRSGRPS_04]

Question 5: Correct

You are the network administrator of a small nonprofit organization. Currently, an employee named Craig Jenkins handles all help desk calls for the organization.

In recent months, the volume of help desk calls has exceeded what Craig can manage alone, so an additional help desk employee has been hired to carry some of the load.

Currently, permissions to network resources are assigned directly to Craig's user object. Because the new employee needs exactly the same level of access, you decide to simply copy Craig's Active Directory domain user object and rename it with the new employee's name.

Will this strategy work?

- (selected) No. Permissions are not copied when a user account is copied.
- Yes. This strategy will be successful.
- No. Making a copy of an existing user causes both accounts to have the same security identifier (SID).
- No. Active Directory does not permit you to copy an existing user account.

Explanation

This strategy won't work. Permissions are not copied when a user object is copied. If the permissions had been assigned to a group that Craig Jenkins was a member of, then the strategy would work because group memberships are preserved when copied.

Active Directory allows you to make copies of existing user accounts. When you do, a new security identifier (SID) is automatically created for the new user.

References

LabSim for Security Pro, Section 8.8.
[All Questions SecPro2017_v6.exm DOM_USRSGRPS_05]

Exam Report: 8.9.10 Practice Questions

Date: 6/20/2019 11:36:27 am
Time Spent: 1:13

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

One of your users, Karen Scott, has recently married and is now Karen Jones. She has requested that her username be changed from *kscott* to *kjones*, but no other values change. Which of the following commands will accomplish this?

- **usermod -u kjones kscott**
- **usermod -u kscott kjones**
- **usermod -l kscott kjones**
- **usermod -l kjones kscott**

Explanation

Use the **usermod** utility to modify user settings. Use the **-l** flag to signal a change to the username. The correct syntax requires the new username value be given, followed by the old username. The **-u** flag changes the UID number.

References

LabSim for Security Pro, Section 8.9.
[All Questions SecPro2017_v6.exm LINUX_USRS_01]

Question 2: Correct

You have performed an audit and have found an active account for an employee with the username joer. This user no longer works for the company.

Which command can you use to disable this account?

- **usermod -d joer**
- **usermod -l joer**
- **usermod -u joer**
- **usermod -L joer**

Explanation

Use **usermod -L joer** to lock the user's password, disabling the account.

usermod -l joer will change the account's login name. **-d** is used for changing the account's home directory. **-u** is for changing the account's numeric ID.

References

LabSim for Security Pro, Section 8.9.
[All Questions SecPro2017_v6.exm LINUX_USRS_02]

Question 3: Correct

An employee named Bob Smith, whose user name is *bsmith*, has left the company. You have been instructed to delete his user account and home directory.

Which of the following commands would produce the required outcome? (Choose all that apply.)

- [ ] **userdel bsmith**
- [x] **userdel bsmith;rm -rf /home/bsmith**
- [ ] **userdel -h bsmith**
- [x] **userdel -r bsmith**

Explanation

userdel -r deletes a user's home directory and user account. The command **userdel** by itself will not delete a user's home directory and user account. Executing **rm -rf** on the user's home directory after executing userdel removes the home directory.

userdel -h displays the syntax and options for the **userdel** command.

References

LabSim for Security Pro, Section 8.9.
[All Questions SecPro2017_v6.exm LINUX_USRS_03]

Question 4: Correct

A user with the account name *larry* has just been terminated from the company. There is good reason to believe that the user will attempt to access and damage files in the system in the very near future.

Which of the following commands will disable or remove the user account from the system and remove his home directory?

- ( ) **userdel larry**
- (•) **userdel -r larry**
- ( ) **userdel -home larry**
- ( ) **userdel -h larry**

Explanation

Use the **userdel** command to delete a user from /etc/passwd and related files that allow access. Use the **-r** option to also remove the home directory.

References

LabSim for Security Pro, Section 8.9.
[All Questions SecPro2017_v6.exm LINUX_USRS_04]

Question 5: Correct

In the /etc/shadow file, which character in the password field indicates that a standard user account is locked?

Explanation

! or !! in the password field of /etc/shadow indicates that the account is locked and cannot be used to log in. The /etc/shadow file holds passwords and password expiration information for

user accounts.

$ preceding the password identifies the password as an encrypted entry. * indicates a system user account entry (which cannot be used to log in).

References

LabSim for Security Pro, Section 8.9.
[All Questions SecPro2017_v6.exm LINUX_USRS_05]

Question 6: Correct

Which of the following utilities could you use to lock a user account? (Select two. Each answer represents an independent solution.)

- [ ] **userdel**
- [ ] **useradd**
- [x] **usermod**
- [x] **passwd**

Explanation

Use the following utilities to lock a user account:

- **passwd -l** disables (locks) an account. This command inserts !! before the password in the /etc/shadow file.
- **usermod -L** disables (locks) an account. This command inserts an ! before the password in the /etc/shadow file.

useradd creates new user accounts, and **userdel** deletes user accounts from the system.

References

LabSim for Security Pro, Section 8.9.
[All Questions SecPro2017_v6.exm LINUX_USRS_06]

Question 7: Correct

You suspect that the *gshant* user account is locked.

Enter the command you use at the command prompt to show the status of the user account.

Explanation

passwd -S gshant displays the status of the gshant user account.

- LK indicates that the user account is locked.
- PS indicates that the user account has a password.

Viewing the /etc/shadow file will also display whether the user account is disabled. The second field for each entry in the /etc/password file is the password field:

- $ preceding the password identifies the password as an encrypted entry.
- ! or !! indicates the account is locked and cannot be used to log in.
- * indicates a system account entry and cannot be used to log in.

References

LabSim for Security Pro, Section 8.9.
[All Questions SecPro2017_v6.exm LINUX_USRS_07]

Exam Report: 8.10.6 Practice Questions

Date: 6/20/2019 12:27:58 pm
Time Spent: 0:47

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 80%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You are the administrator for a small company. You need to add a new group of users to the system. The group's name is sales. Which command will accomplish this?

- **addgroup sales**
- **groupadd -r sales**
- **addgroup -x sales**
- **groupadd sales**

Explanation

Use the **groupadd** utility to add a group to the system. By default, the group will be added with an incrementing number above those reserved for system accounts. If you use the **-r** option, it will add the account as a system account (with a reserved group id number). Because this is a group that is created for users, the **-r** option should not be used.

References

LabSim for Security Pro, Section 8.10.
[All Questions SecPro2017_v6.exm LINUX_GRPS_01]

Question 2: Correct

Due to a merger with another company, standardization is now being imposed throughout the company. As a result of this, the *sales* group must be renamed *marketing*. Which of the following commands will accomplish this?

- **grpchange marketing sales**
- **groupmod -n marketing sales**
- **groupadd -c marketing sales**
- **grpconv marketing sales**

Explanation

Use the **groupmod** utility to modify existing groups. Use the**-n** parameter to change the name of a group to a new text value.

Use the **groupadd** utility to add new groups to the system. Use **grpconv** to add additional security to the group passwords.

References

LabSim for Security Pro, Section 8.10.
[All Questions SecPro2017_v6.exm LINUX_GRPS_02]

Question 3: Correct

You have a group named temp_sales on your system. The group is no longer needed, and you should remove the group. Which of the following commands should you use?

- **groupdel temp_sales**
- **groupmod -R temp_sales**
- **groupmod -n temp_sales**
- **newgroup -R temp_sales**

Explanation

Use **groupdel** to delete a group from the Linux system.

newgroup logs the user in to a group with the group password, but does not contain a **-R** option. **groupmod** modifies the existing group. Be aware of the following options:

- **-A** adds specified users from the group (SUSE distribution).
- **-R** removes specified users from the group (SUSE distribution).
- **-n** changes the name of a group.

References

LabSim for Security Pro, Section 8.10.
[All Questions SecPro2017_v6.exm LINUX_GRPS_03]

Question 4: Correct

You have a group named Research on your system that needs a new password because a member of the group has left the company. Which of the following commands should you use?

- **gpasswd Research**
- **gpasswd research**
- **newpasswd Research**
- **groupmod -p Research**

Explanation

Use **gpasswd Research** to be prompted to enter a new password for the Research group.

Group names are case-sensitive, so **gpasswd research** won't change the password for the Research group. The **groupmod** command does not have a switch that can be used to change passwords. And **newpasswd** is not a valid Linux command.

References

LabSim for Security Pro, Section 8.10.
[All Questions SecPro2017_v6.exm LINUX_GRPS_04]

Question 5: Incorrect

You want to see which primary and secondary groups the dredford user belongs to. Enter the command you would use to display group memberships for dredford.

groups dredford

Explanation

To display the primary and secondary group membership for a specified user account, use the

groups command. In this case, you would enter:
groups dredford

References

LabSim for Security Pro, Section 8.10.
[All Questions SecPro2017_v6.exm LINUX_GRPS_05]

Exam Report: 8.11.4 Practice Questions

Date: 6/20/2019 5:58:12 pm
Time Spent: 1:19

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What is the effect of the following command?

chage -M 60 -W 10 jsmith

- Deletes the *jsmith* user account after 60 days and gives a warning 10 days before it expires.
- Sets the password for *jsmith* to expire after 6 days and gives a warning 10 days before it expires.
- Sets the password for *jsmith* to expire after 6 days and gives a warning 10 days before it expires.
- Sets the password for *jsmith* to expire after 60 days and gives a warning 10 days before it expires.
- Forces *jsmith* to keep the password 60 days before changing it and gives a warning 10 days before changing it.

Explanation

chage -M 60 -W 10 jsmith sets the password for *jsmith* to expire after 60 days and gives a warning 10 days before it expires.

chage sets user passwords to expire. Be aware of the following options:

- **-M** sets the maximum number of days before the password expires.
- **-W** sets the number of days before the password expires that a warning message displays.
- **-m** sets the minimum number of days that must pass after a password change before a user can change the password again.

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_01]

Question 2: Correct

What **chage** command should you use to set the password for *jsmith* to expire after 60 days and give a warning 10 days before it expires? (Tip: Enter the command as if at the command prompt.)

Explanation

chage -M 60 -W 10 jsmith sets the password for *jsmith* to expire after 60 days and gives a warning 10 days before it expires. Use **chage** to set user passwords to expire. Be aware of the following options:

- **-M** sets the maximum number of days before the password expires.
- **-W** sets the number of days before the password expires that a warning message displays.
- **-m** sets the minimum number of days that must pass after a password has been changed before a user can change the password again.

Note: Look in the /etc/shadow file to see current limits for users.

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_02]

Question 3: Correct

Which **chage** option keeps a user from changing their password every two weeks?

- (selected) **-m 33**
- **-a 33**
- **-M 33**
- **-W 33**

Explanation

chage -m 33 forces the user to keep his password for 33 days. This sets the minimum number of days that must pass after a password change before a user can change the password again. Be aware of the other **chage** options:

- **-M** sets the maximum number of days before the password expires.
- **-W** sets the number of days before the password expires that a warning message displays.

chage -a is not a valid option.

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_03]

Question 4: Correct

Which file should you edit to limit the amount of concurrent logins for a specific user? (Tip: Enter the full path to the file.)

Explanation

Use the /etc/security/limits.conf file to limit resource use for all applications. This is from the pam_limits module of the Plugable Authentication Modules (PAM) module set. Entries in /etc/security/limits.conf contain the following:

Entity Type Limit Value

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_04]

Question 5: Correct

Within the /etc/security/limits.conf file, you notice the following entry:

@guests hard maxlogins 3

What effect does this line have on the Linux system?

- ○ Limits the total amount of memory used by the Guest group to 3 MB
- ○ Limits concurrent logins from the same user to three.
- ○ Limits the maximum file size that the Guest group can create to 3GB.
- ➡ ◉ Limits the number of logins from the Guest group to three.

Explanation

@guests hard maxlogins 3 limits the number of logins from the Guest group to three. Use the /etc/security/limits.conf file to limit resource use for all applications. Entries in /etc/security/limits.conf contain the following:

Entity Type Limit Value

jsmith hard fsize 1024 Limits the maximum file size that jsmith can create to 1024 KB.
*** hard maxlogins 1** Limits concurrent logins from the same user to one.
*** soft cpu 10** Sets a soft limit of 10 minutes on the amount of CPU time any single process for any user can take.
rss hard rss 5000 Limits the total amount of memory available to a single user to 5 MB.

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_05]

Exam Report: 8.12.6 Practice Questions

Date: 6/21/2019 10:52:43 am
Time Spent: 0:34

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You want to ensure that all users in the Development OU have a common set of network communication security settings applied.

Which action should you take?

- Create a GPO user policy for the Development OU.
- Create a GPO computer policy for the Computers container.
- Create a GPO folder policy for the folders containing the files.
- Create a GPO computer policy for the computers in the Development OU.

Explanation

Network communication security settings are configured in the Computer Policies section of a GPO.

Built-in containers (such as the Computers container) and folders cannot be linked to a GPO.

References

LabSim for Security Pro, Section 8.12.
[All Questions SecPro2017_v6.exm GPO_OVW_01]

Question 2: Correct

Computer policies include a special category called *user rights*.

Which action does user rights allow an administrator to perform?

- Designate a basic set of rights for all users in an OU.
- Set ACL rights for users on specified computers in an OU.
- Specify the registry settings for all users in an OU.
- Identify users who can perform maintenance tasks on computers in an OU.

Explanation

User rights are a special category of computer policies that identify system maintenance tasks and the users or groups who can perform these actions.

References

LabSim for Security Pro, Section 8.12.
[All Questions SecPro2017_v6.exm GPO_OVW_02]

Question 3: Correct

Which statement is true regarding application of GPO settings?

- If a setting is defined in the Local Group policy on the computer and defined differently in the GPO linked to the OU, the Local Group Policy setting is applied.
- ➡ If a setting is defined in the Local Group policy on the computer and not defined in the GPO linked to the OU, the setting is applied.
- If a setting is defined in the Local Group policy on the computer and not defined in the GPO linked to the OU, the setting is not applied.
- If a setting is not defined in the Local Group policy and is defined in the GPO linked to the OU, the setting is not applied.

Explanation

GPOs are applied in the following order:

1. The Local Group policy on the computer.
2. GPOs linked to the domain that contains the User or Computer object.
3. GPOs linked to the organizational unit(s) that contain(s) the User or Computer objects (from the highest-level OU to the lowest-level OU).

Individual settings within all GPOs are combined to form the effective Group Policy setting as follows:

- If a setting is defined in one GPO and undefined in another, the defined setting is enforced (regardless of the position of the GPO in the application order).
- If a setting is configured in two GPOs, the setting in the last-applied GPO will be used.

References

LabSim for Security Pro, Section 8.12.
[All Questions SecPro2017_v6.exm GPO_OVW_03]

Question 4: Correct

You manage an Active Directory domain. All users in the domain are required by a GPO linked to the domain to use passwords with at least eight characters, but you want to ensure that users in the Administrators OU are required to use passwords with at least 10 characters.

What should you do?

- Create a Local Group policy on the computers used by members of the Administrators OU.
- Create a GPO computer policy for the domain.
- Create a GPO user policy for the Administrators OU.
- ➡ Create a GPO computer policy for the Administrators OU.

Explanation

Password restrictions are configured in the computer policies section of a GPO. Linking this policy to the Administrators OU only applies it to users in that OU because GPOs linked to OUs are applied last.

If Local Group policies are created on the Administrator's computers, they are overwritten by the GPO that is linked to the domain, which only requires users to have passwords with at least eight characters. There is already a GPO computer policy linked to the domain.

References

LabSim for Security Pro, Section 8.12.
[All Questions SecPro2017_v6.exm GRP_POLICY_OVW_04]

Question 5: Correct

You manage an Active Directory domain. All users in the domain have a standard set of internet options configured by a GPO linked to the domain. But you want users in the Administrators OU to have a different set of internet options.

What should you do?

- Create a Local Group policy on the computers used by members of the Administrators OU.
- Create a GPO user policy for the Administrators OU.
- Create a GPO user policy for the domain.
- Create a GPO computer policy for the Administrators OU.

Explanation

Internet options are configured in the User Policies section of a GPO. Linking this policy to the Administrators OU only applies it to users in that OU because GPOs linked to OUs are applied last.

If Local Group policies are created on the Administrator's computers, they are overwritten by the GPO that is linked to the domain, which applies a standard set of internet options to all users in the domain. There is already a GPO user policy linked to the domain.

References

LabSim for Security Pro, Section 8.12.
[All Questions SecPro2017_v6.exm GRP_POLICY_OVW_05]

Exam Report: 8.13.11 Practice Questions

Date: 6/20/2019 7:00:18 pm
Time Spent: 1:22

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following is the single best rule to enforce when designing complex passwords?

- Force use of all four types of characters (uppercase, lowercase, numbers, symbols)
- Computer-generated passwords
- Maximum password age
- Longer passwords

Explanation

The best rule for complex passwords is this: the longer is better. The longer a password is, the harder a password cracking tool must work to break or guess the password.

Computer-generated passwords may be complex, but they are usually difficult to remember. The more difficult a password is to remember, the more likely it is that someone will write it down, making it insecure. Maximum password age is important, but a short password changed often is weaker than a long password that is static for a longer period of time. Requiring the use of all four character types is important, but not as important as overall password length.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_01]

Question 2: Correct

For users on your network, you want to automatically lock user accounts if four incorrect passwords are used within 10 minutes.

What should you do?

- Configure day/time restrictions in the user accounts
- Configure account lockout policies in Group Policy
- Configure the enable/disable feature in the user accounts
- Configure account expiration in the user accounts
- Configure password policies in Group Policy

Explanation

Account lockout disables a user account after a specified number of incorrect login attempts.

The account lockout threshold identifies the number of incorrect login attempts. The account lockout counter identifies a time period for keeping track of incorrect attempts (such as 10 minutes) .
If account lockout locks a user account, use the unlock feature to allow login. Use the enable/disable feature to prevent or allow login using the user account.

Configure account (password) policies in Group Policy to enforce rules about the composition of passwords, such as minimum length, complexity, and history requirements. Use account expiration in a user account to disable an account after a specific day. Use day/time restrictions to prevent login during certain days or hours.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_02]

Question 3: Correct

You want to make sure that all users have passwords over eight characters in length and that passwords must be changed every 30 days.

What should you do?

- (selected) Configure account policies in Group Policy
- Configure expiration settings in the user accounts
- Configure account lockout policies in Group Policy
- Configure day/time settings in the user accounts

Explanation

Configure account (password) policies in Group Policy to enforce rules about the composition of passwords, such as minimum length, complexity, and history requirements.

Use account expiration in a user account to disable an account after a specific day. Use day/time restrictions to prevent login during certain days or hours. Account lockout disables a user account after a specified number of incorrect login attempts.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_03]

Question 4: Correct

You have hired 10 new temporary workers who will be with the company for 3 months.

How can you make sure that these users can only log on during regular business hours?

- Configure account lockout in Group Policy
- Configure account policies in Group Policy
- Configure account expiration in the user accounts
- (selected) Configure day/time restrictions in the user accounts

Explanation

Use day/time restrictions to limit the days and hours when users can log on.

Configure account expiration to disable an account after a specific date. Use account policies in Group Policy to configure requirements for passwords. Use account lockout settings in Group Policy to automatically lock accounts when a specific number of incorrect passwords are entered.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_04]

Question 5: Correct

You are configuring the local security policy of a Windows system. You want to prevent users from reusing old passwords. You also want to force them to use a new password for at least five days before changing it again.

Which policies should you configure? (Select two.)

- [x] Minimum password age
- [ ] Password complexity
- [x] Enforce password history
- [ ] Maximum password age

Explanation

Set the Enforce password history policy to prevent users from reusing old passwords. Set the Minimum password age policy to prevent users from changing passwords too soon. Passwords must remain the same for at least the time period specified.

Use the Maximum password age policy to force periodic changes to the password. After the maximum password age has been reached, the user must change the password. Use the Password complexity to require that passwords include letters, numbers, and symbols. This makes it harder for hackers to guess or crack passwords.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_05]

Question 6: Correct

You are configuring the Local Security policy of a Windows system. You want to require users to create passwords that are at least 10 characters long. You also want to prevent login after three unsuccessful login attempts.

Which policies should you configure? (Select two.)

- [ ] Maximum password age
- [x] Minimum password length
- [x] Account lockout threshold
- [ ] Password complexity
- [ ] Enforce password history
- [ ] Account lockout duration

Explanation

Set the Minimum password length policy to require a password equal to or longer than the specified length. Set the Account lockout threshold policy to lock an account after the specified number of incorrect login attempts.

The following lists explains the incorrect policy choices for this scenario:

- Enforce password history requires users to input a unique (previously unused) password

when changing the password. This prevents users from reusing previous passwords.
• Maximum password age forces users to change the password after the specified time interval.
• Password complexity prevents using passwords that are easy to guess or easy to crack. It forces passwords to include letters, symbols, and numbers, and also requires passwords of at least seven characters. However, you cannot configure a longer password length requirement with this policy.
• Account lockout duration determines the length of time the account is disabled (in minutes). When the time period expires, the account is unlocked automatically.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_06]

Question 7: Correct

You have just configured the password policy and set the minimum password age to 10.

What will be the effect of this configuration?

- (selected) Users cannot change the password for 10 days.
- The password must contain 10 or more characters.
- The previous 10 passwords cannot be reused.
- The password must be entered within 10 minutes of the login prompt being displayed.
- Users must change the password at least every 10 days.

Explanation

The minimum password age setting prevents users from changing the password too frequently. After the password is changed, it cannot be changed again for at least 10 days.

The maximum password age setting determines how frequently a password must be changed. The minimum password length setting controls the minimum number of characters in the password. Password history is used to prevent previous passwords from being reused.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_07]

Question 8: Correct

You have implemented account lockout with a clipping level of 4.

What will be the effect of this setting?

- Incorrect login attempts during the past four hours will be tracked.
- Password hashes will be generated using a salt value of four.
- (selected) The account will be locked after four incorrect attempts.
- Locked accounts will remain locked for four hours.

Explanation

The clipping level specifies the number of incorrect attempts that will trigger account lockout. In this example, four incorrect passwords would lock the user account.

Account lockout duration specifies how long the account remains locked. Incorrect login attempts are typically cleared after a successful login or after a predetermined time passes.

The salt value is a random value that ensures that hashes of the same password result in different hashes.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_08]

Question 9: Correct

Which of the following is **not** an important aspect of password management?

- Prevent use of personal information in a password.
- Always store passwords in a secure medium.
- Enable account lockout.
- Train users to create complex passwords that are easy to remember.

Explanation

Account lockout is not a password management mechanism; rather, it is an access control mechanism to protect against attempted compromise of user accounts.

Password management includes preventing personal information in passwords, training users on how to create complex passwords that are easy to remember, and ensuring that passwords are always stored securely.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_09]

Question 10: Correct

You are teaching new users about security and passwords.

Which of the following is the best example of a secure password?

- T1a73gZ9!
- Stiles_2031
- JoHnSmITh
- 8181952

Explanation

The most secure password is T1a73gZ9! because it is eight or more characters in length and combines upper and lowercase characters, special symbols, and numbers.

The least secure password is 8181952 because it appears to be a birthday. JoHnSmITh is not secure because it is still a name. Stiles_2031 is more secure, but not as secure as random numbers and letters.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_10]

Question 11: Correct

Upon running a security audit in your organization, you discover that several sales employees are using the same domain user account to log in and update the company's customer database.

Which action should you take? (Select two. Each response is a part of a complete solution.)

- [ ] Implement a Group Policy object that implements time-of-day login restrictions.

- [ ] Implement a Group Policy object that restricts simultaneous logins to one.
- [ ] Apply the Group Policy object to the container where the sales user accounts reside.
- [x] Delete the account that the sales employees are currently using.
- [x] Train sales employees to use their own user accounts to update the customer database.

Explanation

You should prohibit the use of shared user accounts. Allowing multiple users to share an account increases the likelihood of the account being compromised. Because the account is shared, users tend to take security for the account less seriously. In the scenario, the following tasks need to be completed:

- The existing shared user account needs to be deleted. Until you delete the account, users will continue to use it for authentication. You could just change the password on the account, but there is a high chance that the new password would be shared again.
- Train sales employees to use their own user accounts to update the customer database. Ensure that these accounts have the level of access required for users to access the database.

Applying time of day or concurrent logon restrictions in a Group Policy object will not address the issue in this scenario.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_11]

Exam Report: 8.14.7 Practice Questions

Date: 6/21/2019 10:25:30 am
Time Spent: 0:49

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and computer accounts have been moved into their corresponding OUs.

You define a password and account lockout policy for the domain. However, members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You need to make the change as easily as possible. Which should you do?

- Create a new domain. Move the contents of the Directors OU to the new domain. Configure the necessary password policy on the domain.
- Implement a granular password policy for the users in the Directors OU.
- Create a GPO linked to the Directors OU. Configure the password policy in the new GPO.
- In Active Directory Users and Computers, select all user accounts in the Directors OU. Edit the user account properties to require the longer password.

Explanation

Use granular password policies to force different password policy requirements for different users.

Password and account lockout policies are enforced only in GPOs linked to the domain, not to individual OUs. Prior to Windows Server 2008, the only way to configure different password policies was to create a different domain.

References

LabSim for Security Pro, Section 8.14.
[All Questions SecPro2017_v6.exm SMART_CARD_AUTH_01]

Question 2: Correct

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and computer accounts have been moved into their corresponding OUs. You define a password and account lockout policy for the domain. However, members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You would like to define a granular password policy for these users. Which tool should you use?

- Active Directory Sites and Services

- ADSI Edit
- Active Directory Domains and Trusts
- Active Directory Users and Computers
- Group Policy Management Console and Group Policy Management Editor

Explanation

Use ADSI Edit or the Active Directory module for Windows PowerShell to define granular password policies.

Use Group Policy Management Console and Group Policy Management Editor to define password policies for an entire domain.

References

LabSim for Security Pro, Section 8.14.
[All Questions SecPro2017_v6.exm SMART_CARD_AUTH_02]

Question 3: Correct

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and computer accounts have been moved into their corresponding OUs. You define a password and account lockout policy for the domain. However, members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You need to make the change as easily as possible. Which should you do?

- Create a granular password policy. Apply the policy to the Directors OU.
- Create a granular password policy. Apply the policy to all users in the widgets.com domain.
- Create a granular password policy. Apply the policy to all users in the Directors OU.
- Create a granular password policy. Create a distribution group. Apply the policy to the group. Add all users in the Directors OU to the group.

Explanation

To use granular password policies:

- Create the Password Settings Object (PSO) with the necessary settings
- Edit the msDS-PSOAppliesTo property in the PSO to identify the users or global security groups to which the policy applies
- If the policy was applied to a group, add members to the group

The msDS-PSOAppliesTo property in the PSO identifies the users to which the policy applies. Using ADSI Edit, you can apply the policy to any object. However, only policies applied to user accounts or global security groups will be effective. To apply a policy to all users in an OU, add each user to the msDS-PSOAppliesTo property or use a global security group. Granular password policies cannot be applied to an email distribution group.

References

LabSim for Security Pro, Section 8.14.
[All Questions SecPro2017_v6.exm SMART_CARD_AUTH_03]

Question 4: Correct

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and computer

accounts have been moved into their corresponding OUs. Members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You define a new granular password policy with the required settings. All users in the Directors OU are currently members of the DirectorsGG group, a global security group in that OU. You apply the new password policy to that group. Matt Barnes is the chief financial officer. He would like his account to have even more strict password policies than is required for other members in the Directors OU.

What should you do?

- Edit the existing password policy. Define exceptions for the required settings. Apply the exceptions to Matt's user account.
- Create a granular password policy for Matt. Create a new group and make Matt a member of the group. Apply the new policy directly to the new group. Make sure the new policy has a higher precedence value than the value for the existing policy.
- Create a granular password policy for Matt. Apply the new policy directly to Matt's user account.
- Create a granular password policy for Matt. Apply the new policy directly to Matt's user account. Remove Matt from the DirectorsGG group.

Explanation

To use a different set of policies for a specific user, create a PSO for the user and apply it directly to the user account. If a PSO has been applied directly to a user, that PSO is in effect, regardless of the precedence value.

You could create a second group only for Matt's account and password policy. However, this policy must have a lower precedence value than the value set for the policy applied to the DirectorsGG group. Removing Matt's account from the DirectorsGG group is unnecessary and would probably affect his permissions to network resources.

References

LabSim for Security Pro, Section 8.14.
[All Questions SecPro2017_v6.exm SMART_CARD_AUTH_04]

Question 5: Correct

Match each smart card attack on the left with the appropriate description on the right.

Software Attacks
- Exploiting vulnerabilities in a card's protocols or encryption methods

Eavesdropping
- Capturing transmission data produced by a card as it is used

Fault Generation
- Deliberately inducing malfunctions in a card

Microprobing
- Accessing the chip surface directly to observe, manipulate, and interfere with a circuit

Explanation

Smart cards are subject to the following weaknesses:

- *Microprobing* is the process of accessing the chip surface directly to observe, manipulate, and interfere with the circuit.
- *Software attacks* exploit vulnerabilities in the card's protocols or encryption methods.

- *Eavesdropping* captures transmission data produced by the card as it is used.
- *Fault generation* deliberately induces malfunctions in the card.

References

LabSim for Security Pro, Section 8.14.
[All Questions SecPro2017_v6.exm SMART_CARD_AUTH_05]

Question 6: Correct

Which of the following is **not** true of smart cards?

- (selected) Smart cards a powered internally by a small battery.
- Smart cards have their own processor, allowing the card itself to perform its own cryptographic functions.
- Smart cards use PKI technology to store digital signatures, cryptography keys, and identification codes.
- Smart cards are generally considered to be tamper-proof.

Explanation

Smart cards are not powered internally by a small battery; they are powered externally by the smart card reader.

Smart cards are plastic credit card-sized cards with an embedded memory chip that contains encrypted authentication information. Be aware that smart cards:

- Use PKI technology to store digital signatures, cryptography keys, and identification codes.
- Can authenticate a user when used in conjunction with a smart card reader connected to a computer system.
- Typically have up to 8 KB of RAM, 346 KB of ROM, 256 KB of programmable ROM, and a 16-bit microprocessor integrated within the card itself.
- Have their own processor, allowing the card itself to perform its own cryptographic functions.
- Use a serial interface to connect to the card reader.
- Are generally considered to be tamper-proof.
- Can be classified into two categories:
  - *Contact smart cards* use a gold-plated contact pad that must physically touch the contact pad on a smart card reader.
  - *Contactless smart cards* do not require physical contact with the reader device. Instead, these cards use RFID technology to communicate with the smart card reader. An antenna is wound around the edge of card and activated when the card is within proximity of the card reader.

References

LabSim for Security Pro, Section 8.14.
[All Questions SecPro2017_v6.exm SMART_CARD_AUTH_06]

Exam Report: 9.1.6 Practice Questions

Date: 6/21/2019 11:49:48 am
Time Spent: 1:31

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

The government and military use the following information classification system:

- Unclassified
- Sensitive but unclassified
- Confidential
- Secret
- Top secret

Drag the classification on the left to the appropriate description on the right.

The lowest level of classified information used by the military. Release of this information could cause damage to military efforts.

✔ Confidential

If this information is released, it poses grave consequences to national security.

✔ Top secret

This information can be accessed by the public and poses no security threat.

✔ Unclassified

If this information is disclosed, it could cause some harm, but not a national disaster.

✔ Sensitive but unclassified

If this information is disclosed, it could cause severe and permanent damage to military actions.

✔ Secret

Explanation

The government and military use the following information classification system:

- **Unclassified**: information that can be accessed by the public and poses no security threat.
- **Sensitive but unclassified**: information that, if disclosed, could cause some harm, but not a national disaster.
- **Confidential**: information that is the lowest level of classified information used by the military. It allows restriction of release of information under the Freedom of Information Act. Release of this information could cause damage to military efforts.
- **Secret**: information that, if disclosed, could cause severe and permanent damage to military actions.
- **Top Secret**: information that is the highest level of classified information used by the

military. If top secret information is released, it poses a grave threat to national security.

References

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_02]

Question 2: Correct

Which of the following government acts protects medical records and personal health information?

- FACTA
- FISMA
- ACA
- HIPAA

Explanation

In the US, you must follow laws dictated by three government acts:

- **HIPAA** stands for Health Insurance Portability and Accountability Act. HIPAA protects medical records and personal health information. Companies that provide healthcare insurance handle HIPAA-protected information. And, of course, companies that provide health-related services also handle HIPAA-protected information.
- **FACTA**, the Fair and Accurate Credit Transactions Act, was created to protect against identity theft. It applies to the disposal of consumer reports and related information. FACTA includes credit reports, credit scores, employment history information, check writing history, insurance claims, residential or tenant history, and medical history. Every business handles FACTA-protected information, and every business must comply with FACTA laws.
- **FISMA**, the Federal Information Security Management Act, protects government information. It is primarily concerned with proper data destruction and has detailed disposal requirements.
- **ACA** is the Affordable Care Act, often referred to as Obamacare.

References

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_06]

Question 3: Correct

Many organizations use the Information Security Classification Framework, which uses the following classifications:

- High
- Medium
- Low

Drag the sensitivity classification on the left to the appropriate description on the right. (Classifications may be used once, more than once, or not at all.)

Could cause personal hardship or embarrassment.

✔ Medium

Could cause personal embarrassment or inconvenience.

✔ Low

Could cause loss of life or social hardship.

✔ High

Could cause operational harm such as loss of control or loss of public trust.

✔ High

Could cause operational harm such as loss of confidence or damage to reputation.

✔ Medium

Explanation

Many organizations use the Information Security Classification Framework, which has the following sensitivity classifications:

- **High**: could cause extremely serious personal or organizational injury, including:
  - Extreme financial loss
  - Extreme operational harm, such as loss of control or loss of public trust
  - Extreme personal harm, such as loss of life or social hardship
- **Medium**: could cause serious personal or organizational injury, including:
  - Significant financial loss
  - Significant operational harm, such as loss of confidence or damage to reputation
  - Significant personal harm, such as personal hardship or embarrassment
- **Low**: could cause limited or no injury to individuals or the organization, including:
  - Limited financial loss
  - Limited operational harm, such as reduced organizational effectiveness or loss of morale
  - Limited personal harm, such as embarrassment or inconvenience

References

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_01]

Question 4: Correct

Which of the following data destruction techniques uses a punch press or hammer system to crush a hard disk?

- ○ Purging
- ○ Shredding
- ➡ ◉ Pulverizing
- ○ Pulping
- ○ Degaussing

Explanation

The following are various ways to destroy data:

- **Burning**: the method of building a small fire somewhere legal and safe. Use metal tongs to burn your documents one by one or a few at a time. It's important to ensure that each document is turned into ash—if sensitive information escapes the flames and flies away, it might fall into the wrong hands.
- **Shredding**: running a hard disk through a disk shredder, physically destroying the drive.
- **Pulping**: a way of removing all traces of ink from paper by using chemicals and then mashing the paper into pulp. Since these chemicals can ruin carpet and clothing, you should perform this process outside and use protective gloves.
- **Pulverizing**: this technique is like shredding, except that it uses a punch press or hammer system to crush a hard disk into a pile of metal confetti.
- **Degaussing**: purges the hard disk by exposing it to a high magnetic pulse that destroys

all of the data on the disk. It also ruins the motors inside the drive.
• **Purging**: the removal of sensitive data, ensuring that the data cannot be reconstructed by any known technique.
• **Wiping**: is a software-based method of overwriting data to completely destroy all electronic data residing on a hard disk drive or other digital media. Wiping uses zeros and ones to overwrite data onto all sectors of the device. The data is rendered unrecoverable and achieves data sanitization.

References

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_05]

Question 5: Correct

If you lose your wallet or purse and it ends up in the wrong hands, several pieces of information could be used to do personal harm to you. These pieces of information include the following:

- Name and address
- Driver license number
- Credit card numbers
- Date of birth

Which of the following classifications does this information fall into?

- ○ Private internal information
- ○ Private restricted information
- ➡ ◉ Personally identifiable information
- ○ Proprietary information

Explanation

Personally identifiable information (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. This includes:

- Full name (if not common)
- Home address
- Email address (if private from an association/club membership, et cetera)
- National identification number
- Passport number
- IP address (when linked, but it is not PII by itself in US)
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Telephone number
- Login name, screen name, nickname, or handle

Proprietary information is information that a company wishes to keep confidential. Private internal information is restricted to individuals within the organization and can include personnel records, financial records, and customer lists. Private restricted information is restricted to limited authorized personnel within the organization and can include trade secrets, strategic information, and highly sensitive information.

References

LabSim for Security Pro, Section 9.1.

[All Questions SecPro2017_v6.exm DATA_MAN_03]

Question 6: Correct

When you dispose of a computer or sell used hardware and it is crucial that none of the data on the hard disks can be recovered.

Which of the following actions can you take to ensure that no data is recoverable?

- (selected) Damage the hard disks so badly that all data remanence is gone.
- Delete all files from all the hard disks in the computer.
- Reformat all the hard disks in the computer.
- Encrypt all the data on the hard disks.

Explanation

When you dispose of a computer, sell used hardware, or erase important information, it's crucial to destroy all of the data on a device. It's not enough to delete the data. Reformatting the hard drive is not sufficient. If other people can access the computer, they can use data remanence, the residual representation of erased data, to recover information. You must damage the hardware so badly that the remanence is gone.

References

LabSim for Security Pro, Section 9.1.
[All Questions SecPro2017_v6.exm DATA_MAN_04]

Exam Report: 9.2.5 Practice Questions

Date: 6/21/2019 11:46:31 am
Time Spent: 1:46

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You want email sent from users in your organization to be encrypted to make messages more secure.

Which of the following is an option you can use to enhance the encryption of email messages?

- A hashing service provider
- A symmetric key exchange
- An asymmetric key exchange
- A cryptographic service provider

Explanation

Cryptographic service providers (CSPs) are software libraries that can be used to enhance encryption. Applications can use these to help secure email and provide strong user authentication.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_01]

Question 2: Correct

Advanced cryptography includes various modes of operation.

Drag the mode of operation on the left to the appropriate definition on the right.

Each cipher text block is fed back into the encryption and then encrypts the next plaintext block.

✓ Cipher Feedback Mode

Each plaintext block is added to the previous cipher text block and then the result is encrypted with the key.

✓ Cipher Block Chaining Mode

This mode can encrypt or decrypt one fixed-length block.

✓ Block Cipher Mode

Sender and recipient access a reliable counter that computes a new shared value each time a cipher text block is exchanged.

✓

Counter Mode

Feeds the output blocks back to the block cipher.

✓ Output Feedback Mode

Explanation

Advanced cryptography includes the following modes of operation:

- **Block Cipher Mode**: This mode provides confidentiality and authenticity services. It can encrypt or decrypt one fixed-length block. It works on large chunks of data at a time, often combining blocks for additional security. Block ciphers are more useful when the amount of data is known.
- **Cipher Block Chaining Mode**: Each plaintext block is added to the previous cipher text block, and then the result is encrypted with the key.
- **Cipher Feedback Mode**: Each cipher text block is fed back into the encryption to then encrypt the next plaintext block.
- **Output Feedback Mode**: This mode feeds the output blocks back to the block cipher. These blocks then make strings of bits to feed the encryption algorithm, acting as the key generator.
- **Counter Mode**: Both the sender and recipient will access a reliable counter that computes a new shared value each time a cipher text block is exchanged. The counter needs to be synchronized between both parties.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_03]

Question 3: Correct

If a message sender encrypts a message with a key and a message receiver decrypts it using the same key, which type of key exchange is taking place?

- Digital signature
- Counter mode
- Asymmetric
- ➡ Symmetric

Explanation

A symmetric key is when the sender uses a public key to encrypt a message and the recipient uses that same public key to decrypt it.

An asymmetric key is where the sender's and the receiver's keys are different for the encrypting and decrypting processes. Using counter mode, both the sender and recipient access a reliable counter that computes a new shared value each time a cipher text block is exchanged. A digital signature is a mathematical scheme for demonstrating the authenticity of digital message or document.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_02]

Question 4: Correct

At the end of the cryptographic process, output is generated. With one type of output, simple character changes in the plaintext will cause several characters to change in the cipher text.

What type of output is this?

- Hashing

- Diffusion
- Encryption
- Collision

Explanation

At the end of the cryptographic process, output is generated:

- Simple character changes in the plaintext will cause several characters to change in the cipher text. This is called a diffusion.
- When two different inputs to a function produce the same output, it is called a collision. They are not common, but can occur.
- A digital signature is a mathematical scheme for demonstrating the authenticity of digital message or document. A valid digital signature gives a message credibility, guaranteeing the recipient that the message has not been tampered with in transit.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_05]

Question 5: Correct

Drag the cryptographic algorithm on the left to the appropriate explanation on the right. (Each algorithm may be used once, more than once, or not at all.)

Generates two different yet mathematically related keys.

✓ Asymmetric

Only the private key can be used to decrypt information.

✓ Asymmetric

Generates a single key that is used for both encryption and decryption.

✓ Symmetric

Algorithm used for signature verification and data integrity checking.

✓ Hashing

The public key can only be used to encrypt information.

✓ Asymmetric

Explanation

Cryptographic algorithms are as follows:

- **Symmetric**: Generates a single key that is used for both encryption and decryption. If the key were to fall in the wrong hands, messages encrypted with the key both past and future can be decrypted.
- **Asymmetric**: Generates two different yet mathematically related keys. The encryption key can be shared publicly. This is because the public key is used only to encrypt information; it cannot decrypt information at all. The only key that can decrypt the information is the private key.
- **Hashing**: Instead of being used to encrypt information, keys are used for signature verification and data integrity checking. They take a string of characters of an undetermined length and convert it into a string of characters that has a specific length. This output is known as a digest. Hashes should not be able to be reconstructed from the output of the hash function.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_04]

Exam Report: 9.3.4 Practice Questions

Date: 6/21/2019 11:44:11 am
Time Spent: 0:43

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 83%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What is the main function of a TPM hardware chip?

- Generate and store cryptographic keys
- Control access to removable media
- Provide authentication credentials on a hardware device
- Perform bulk encryption in a hardware processor

Explanation

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard that stores and generates cryptographic keys. These keys are used for encryption and authentication, but the TPM does not perform the actual encryption.

A smart card is a hardware device containing a digital certificate. The smart card can be used for authentication. Special hardware processors perform bulk encryption in hardware, rather than software. These processors typically encrypt data using AES or encrypt network traffic using IPSec.

References

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_01]

Question 2: Correct

Which of the following functions are performed by the TPM?

- Create a hash of system components
- Provide authentication credentials
- Encrypt network data using IPSec
- Perform bulk encryption

Explanation

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard and stores and generates cryptographic keys. The TPM also generates hash values of system components. The hash value verifies that startup components have not been modified. Because each system will have a unique hash value, the hash can also be used as a form of identification for the system.

Keys generated by the TPM are used for encryption and authentication, but the TPM does not perform the actual encryption. A smart card is a hardware device containing a digital certificate. The smart card can be used for authentication. Special hardware processors perform bulk encryption in hardware, rather than software. These processors typically encrypt data using AES or encrypt network traffic using IPSec.

References

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_02]

Question 3: Correct

Which of the following is a direct protection of integrity?

- Digital envelope
- Asymmetric encryption
- Symmetric encryption
- ➡ Digital signature

Explanation

A digital signature is a direct protection of integrity, as it includes the use of hashing, which detects changes to integrity.

Digital envelopes, symmetric encryption, and asymmetric encryption do not provide direct integrity protection, nor do they use hashing to provide integrity protection.

References

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_03]

Question 4: Correct

What is the most obvious means of providing non-repudiation in a cryptography system?

- Shared secret keys
- Hashing values
- Public keys
- ➡ Digital signatures

Explanation

Digital signatures, which are private keys from an asymmetric cryptographic system, are the most obvious means of providing non-repudiation. Only a single person is in possession of their private key. If a message is found with their digital signature, then they are the only user who could possibly have created and transmitted it.

Public keys are useful for restricting delivery, such as using them as digital envelopes, but they don't provide for non-repudiation. Hashing values protect integrity, but they don't provide non-repudiation. Shared secret keys do not provide true non-repudiation because two entities hold copies of the shared key.

References

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_04]

Question 5: Correct

When a sender encrypts a message using their own private key, what security service is being

provided to the recipient?

- Availability
- Confidentiality
- Integrity
- Non-repudiation

Explanation

When a sender encrypts a message using their own private key, the security service of non-repudiation is being provided to the recipient. The encrypted message can be freely decrypted using the public key. Because only the sender knows the private key, encrypting the message with the private key proves that only the sender could have sent the message.

Integrity is provided when hashing is used. Because the public key is freely available, the encryption does not provide confidentiality (anyone with the public key could read the message contents). Availability is not provided by any form of cryptography.

References

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_05]

Question 6: Incorrect

Which of the following statements is **true** when comparing symmetric and asymmetric cryptography?

- ~~Asymmetric key cryptography is quicker than symmetric key cryptography while processing large amounts of data.~~
- Asymmetric key cryptography is used to distribute symmetric keys.
- Symmetric key cryptography uses a public and private key pair.
- Symmetric key cryptography should be used for large, expanding environments.

Explanation

Asymmetric key cryptography can be used to distribute symmetric keys. This is known as a *hybrid* cryptography system. A hybrid cryptography system combines the strengths of both the symmetric and asymmetric cryptography systems (meaning that symmetric systems can process large amounts of data relatively fast, and asymmetric systems can securely distribute keys).

Symmetric cryptography uses a single key pair, with each partner using the same key. Asymmetric cryptography uses a public and a private key pair. Symmetric key cryptography processing is about 1000 times faster than asymmetric cryptography. In large, expanding environments, managing keys with symmetric key cryptography is difficult.

References

LabSim for Security Pro, Section 9.3.
[All Questions SecPro2017_v6.exm CRYPTO_IMPL_06]

Exam Report: 9.4.3 Practice Questions

Date: 6/21/2019 9:04:48 pm
Time Spent: 3:49

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 93%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

If a birthday attack is successful, meaning the attacker discovers a password that generates the same hash as that captured from a user's login credentials, which of the following is true? (Select two.)

- [ ] The discovered password is always the same as the user's password.
- [ ] The user is forced to change their password at their next login attempt.
- [x] The discovered password will allow the attacker to log in as the user, even if the discovered password is not the same as the user's password.
- [x] A collision was discovered.

Explanation

The discovered password will allow the attacker to log on as the user, even if the discovered password is not the same as the user's password. This is because the birthday attack (password cracking) will discover a collision. A collision is when two messages produce the same hash. A collision does not guarantee that the two messages are the same. Therefore, another password could be discovered that has the same hash as the original user's password. Since the authentication system checks only for matching hashes, the attacker could log on with a different password as long as it produces the correct hash.

The discovered password might not be the same as the user's password, since collision only ensures that two messages produce the same hash, not that the two messages are the same. The attack component of the birthday attack is collision, not collusion. Collusion is when two or more people agree to work together to commit a security violation. The act of an attacker discovering a user's password does not automatically force the user to change their password upon the next login attempt. Instead, this is a good security practice to implement if the security team discovers or suspects a password compromise.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_14]

Question 2: Correct

Which of the following is a mathematical attack that targets the complexity of a cryptosystem's algorithm?

- ( ) Birthday attack
- ( ) Replay attack
- (•)

- Analytic attack
- Brute force attack

Explanation

An analytic attack is a mathematical that targets the complexity of a cryptosystem's algorithm. The goal of an analytic attack is to break the algorithm.

A birthday attack is focused on hashing algorithms, but not on the algorithm itself. Instead, a birthday attack exploits a statistical anomaly of collusion when two different messages using the same algorithm produce the same message digest. A brute force attack tries all possible combinations of keys to decipher an encrypted message. A replay attack attempts to re-transmit encryption session keys in hopes of accessing the resource in a de-encrypted mode.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_01]

Question 3: Correct

When an attacker decrypts an encoded message using a different key than was used during encryption, what type of attack has occurred?

- Statistical
- Key clustering
- Analytic
- Replay

Explanation

A *key clustering* attack is where the attacker decrypts an encoded message using a different key than was used during encryption.

A statistical attack exploits weaknesses in a cryptosystem, such as inability to produce random numbers or floating point errors. An analytic attack uses an algebraic manipulation to reduce the complexity of the algorithm. A replay attack attempts to re-transmit encryption session keys in hopes of accessing the resource in a de-encrypted mode.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_06]

Question 4: Correct

Which of the following is an example of a statistical attack against a cryptosystem?

- Exploiting a computer's inability to produce random numbers
- Intercepting messages between two communication partners and modifying the content
- Attempting every possible key pattern
- Exploiting faulty implementation of an algorithm in software

Explanation

An example of a statistical attack against a cryptosystem is exploiting a computer's inability to produce true random numbers. Another example is to exploit the floating point errors in a processor. A computer system's inability to produce true random numbers makes the possibility of the re-use of keys probable, if not likely.

Attempting every possible key pattern is a form of brute force attack. Exploiting faulty

implementation of an algorithm in software is an implementation attack. Intercepting messages between two communication partners and modifying the content is a form of man-in-the-middle attack.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_02]

Question 5: Correct

Which of the following is **not** a countermeasure against dictionary attacks?

- Avoiding industry acronyms
- Using short passwords
- Using three or four different keyboard character types (lowercase, uppercase, numerals, and symbols)
- Avoiding common words

Explanation

Using short passwords is not a direct countermeasure against dictionary attacks. All too often, a short password is a simple common word. A dictionary attack is designed to quickly discover passwords that use common words. Dictionary attacks can be customized for the intended victim. If the attacker knows a few details about the victim, such as hobbies, sports interests, education, or industry, then the dictionary can be customized to focus on words, terms, and acronyms related to those topics.

Avoiding common words, using three or four different keyboard character types, and avoiding industry acronyms are all good countermeasures against dictionary attacks.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_12]

Question 6: Correct

Which of the following password attacks adds appendages to known dictionary words?

- Dictionary
- Hybrid
- Analytic
- Brute force

Explanation

A *hybrid* attack adds appendages to known dictionary words (for example, 1password, password07, and p@ssword1).

A *brute force* attack works through all possibilities until the password is cracked. A *dictionary* attack tries known words (such as from a dictionary). An *analytic* attack uses an algebraic manipulation to reduce the complexity of the algorithm.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_08]

Question 7: Correct

Which type of password attack employs a list of pre-defined passwords that it tries against a login prompt or a local copy of a security accounts database?

- Dictionary
- Salami
- Asynchronous
- Brute force

Explanation

A dictionary attack is a type of password attack that employs a list of pre-defined passwords that it tries against a login prompt or a local copy of a security accounts database. A dictionary attack is designed to quickly discover passwords that use common words. Dictionary attacks can be customized for the intended victim. If the attacker knows a few details about the victim, such as hobbies, sports interests, education, or industry, then the dictionary can be customized to focus on words, terms, and acronyms related to those topics.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_10]

Question 8: Correct

Which form of cryptanalysis focuses on weaknesses in software, the protocol, or the encryption algorithm?

- Implementation attack
- Ciphertext only attack
- Statistical attack
- Analytic attack

Explanation

An implementation attack exploits implementation weaknesses, such as in software, the protocol, or the encryption algorithm.

A statistical attack exploits weaknesses in the computing platform, such as the inability to produce random numbers or CPU floating point errors. An analytic attack focuses on weaknesses in the algorithm itself. A ciphertext only attack is a solution attack where material supplied by the attacker is decrypted by the victim, revealing the key.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_03]

Question 9: Correct

Why are brute force attacks always successful?

- They are platform independent.
- They can be performed in a distributed parallel processing environment.
- They are fast.
- They test every possible valid combination.

Explanation

Brute force attacks are always successful because they test every possible valid combination. Thus, they will eventually discover the actual key, password, or code that was used.

Brute force attacks are not fast, they are usually platform and application-specific, and while they can be deployed in distributed parallel processing environments in order to make them faster, this does not necessarily make them successful.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_11]

Question 10: Correct

Your company produces an encryption device that lets you enter text and receive encrypted text in response. An attacker obtains one of these devices and starts inputting random plaintext to see the resulting ciphertext.

Which type of attack is this?

- Chosen cipher
- Chosen plaintext
- Brute force
- Known plaintext

Explanation

A *chosen plaintext* attack is where the attacker chooses the plaintext to be encrypted. This event can occur when a worker steps away from the computer and the attacker sends a message and captures the resulting cipher text. The attacker can select plaintext that will produce clues to the encryption key used.

A brute force attack is where the attacker tries every known combination. A chosen ciphertext is where the attacker produces ciphertext and then sends it through a decryption process to see the resulting plaintext. A known plaintext attack is where an attacker has seen the plaintext and the resulting ciphertext.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_05]

Question 11: Correct

If two different messages or files produce the same hashing digest, then a collision has occurred. Which form of cryptographic attack exploits this condition?

- Meet-in-the-middle attack
- Statistical attack
- Adaptive chosen ciphertext attack
- Birthday attack

Explanation

Birthday attacks exploit collisions. Birthday attacks exploit the probability that two messages using the same hash algorithm will produce the same message digest.

An adaptive chosen ciphertext attack is used to discover the encryption key. A meet-in-the-middle-attack is used to determine the algorithm used. A statistical attack is used to exploit computer-based cryptosystems, such as the inability to produce true random numbers.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_13]

Question 12: Correct

Which of the following best describes a side-channel attack?

- The attack exploits weaknesses in a cryptosystem, such as inability to produce random numbers or floating point errors.
- ➡ The attack is based on information gained from the physical implementation of a cryptosystem.
- The attack targets a weakness in the software, protocol, or encryption algorithm.
- The attack targets the key containing a small data set.

Explanation

A *side-channel* attack is where an attack is based on information gained from the physical implementation of a cryptosystem rather than theoretical weaknesses in the algorithms, such as the length of time required during encryption or decryption.

A *mathematical* attack is an attack on a key containing a small data set. An *implementation* attack exploits implementation weaknesses, such as in software, the protocol, or the encryption algorithm. A *statistical* attack exploits weaknesses in a cryptosystem, such as inability to produce random numbers or floating point errors.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_07]

Question 13: Correct

In which type of attack does the attacker have access to both the plaintext and the resulting cipher text, but does not have the ability to encrypt the plain text?

- Chosen cipher
- Brute force
- ➡ Known plaintext
- Chosen plaintext

Explanation

A *known plaintext* attack is where an attacker has seen the plaintext and the resulting cipher text. The attacker can make conclusions about the encrypting key and will have validation if the encrypting key is discovered.

A chosen plaintext attack is where the attacker chooses the plaintext to be encrypted. The main difference between known plaintext and chosen plaintext is the attacker's ability to select random plaintext and run it through the encrypting mechanism.

A brute force attack is where the attacker tries every known combination. A chosen cipher text is where the attacker produces cipher text and then sends it through a decryption process to see the resulting plaintext.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_04]

Question 14: Incorrect

Which of the following attacks typically takes the longest amount of time to complete?

- Dictionary attack
- Brute force attack
- ~~Impersonation attack~~
- Replay attack

Explanation

A brute force attack typically takes the longest amount of time. A brute force attack is a form of attack that attempts every possible key or password pattern for a message, login prompt, or security file. To combat or protect against brute force attacks, always use strong, complex passwords and wisely use the keyspace of your cryptosystems.

A dictionary attack, replay attack, and impersonation attack all take considerably less time than a brute force attack and are often used as shortcuts to a brute force attack.

References

LabSim for Security Pro, Section 9.4.
[All Questions SecPro2017_v6.exm CRYPTO_ATT_09]

Exam Report: 9.5.4 Practice Questions

Date: 6/21/2019 9:10:50 pm
Time Spent: 1:29

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following are true of Triple DES (3DES)? (Select two.)

- [ ] Uses the Rijndael block cipher
- [x] Is used in IPsec
- [ ] Can easily be broken
- [x] Uses a 168-bit key
- [ ] Uses 64-bit blocks with 128-bit keys

Explanation

Triple DES:

- Applies DES three times
- Uses a 168-bit key
- Used in IPsec as its strongest and slowest encipherment

Advanced Encryption Standard (AES) uses the Rijndael block cipher. DES can easily be broken. International Data Encryption Algorithm (IDEA) uses 64-bit blocks with 128-bit keys.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_01]

Question 2: Correct

Which of the following is the most frequently used symmetric key stream cipher?

- (x) Ron's Cipher v4 (RC4)
- ( ) Blowfish
- ( ) Advanced Encryption Standard (AES)
- ( ) Ron's Cipher v2 (RC2)

Explanation

RC4 is the most frequently used symmetric key stream cipher. RC4 is commonly used with WEP and SSL.

AES, RC2, and Blowfish are all symmetric *block* ciphers.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_02]

Question 3: Correct

Which of the following forms of cryptography is best implemented in hardware?

- Public key
- Asymmetric
- Symmetric block
- Symmetric stream

Explanation

Symmetric stream cryptography is best implemented in hardware because the data size makes it infeasible to have enough RAM or CPU cycles to process the data.

Symmetric block cryptography is primarily implemented in software. Asymmetric cryptography, also known as public key cryptography, is mainly used for key distribution, digital signatures, and data encryption for small amounts of data.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_03]

Question 4: Correct

Which of the following symmetric block ciphers does **not** use a variable block length?

- Elliptic Curve (EC)
- Ron's Cipher v5 (RC5)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)

Explanation

International Data Encryption Algorithm (IDEA) does not use variable block lengths. In addition to IDEA, the following symmetric block ciphers also do not use variable block lengths:

- Data Encryption Standard (DES)
- Ron's Cipher v2 or Ron's Code v2 (RC2)
- Blowfish
- Twofish
- SkipJack

AES uses variable block lengths. RC5 uses 32-, 64- or 128-bit block lengths. Elliptic Curve (EC) is an asymmetric cipher.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_05]

Question 5: Correct

Which of the following encryption mechanisms offers the least security because of weak keys?

- AES

- (selected) DES
- TwoFish
- IDEA

Explanation

DES offers the least encryption security from the cryptography systems in this list. DES has a limitation of 56-bit keys, the weakest of those listed here. The strength of a cryptosystem lies not only in long keys but in the algorithm, initialization vector or method, the proper use of the keyspace, and the protection and management of keys.

AES (128, 192, 256 bit keys), TwoFish (up to 256 bit keys), and IDEA (128 bit keys) all support stronger keys than DES.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_06]

Question 6: Correct

Which version of the Rivest cipher is a block cipher that supports variable bit length keys and variable bit block sizes?

- (selected) RC5
- RC4
- RSA
- RC2

Explanation

RC5 is a block cipher that supports variable bit length keys and variable bit block sizes.

RC4 is a stream cipher. RC2 is limited to 64 bit blocks. RSA is not a Rivest cipher; rather, it is an asymmetric cryptography system developed by the same organization.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_07]

Question 7: Correct

Which of the following symmetric cryptography systems does not support a variable block size?

- Rijndael
- (selected) IDEA
- AES
- RC5

Explanation

IDEA is a symmetric cryptography system that does not support a variable block size. IDEA only supports a 64-bit block size.

RC5, AES, and AES's algorithm Rijndael all support variable block sizes. RC5's supported block sizes are 32, 64, and 128. AES (Rijndael) supports any block size.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_10]

Question 8: Correct

You want to encrypt data on a removable storage device. Which encryption method would you choose to use the strongest method possible?

- (selected) AES
- SHA-1
- RSA
- 3DES

Explanation

AES is stronger and faster than 3DES when implemented with a large key size (256-bits). DES was one of the first symmetric encryption methods and is now obsolete (known weaknesses can be used to break the encryption). 3DES improves upon DES by applying the encryption three times. It is an acceptable alternative to DES.

RSA is an asymmetric encryption algorithm. Asymmetric encryption is not typically used for bulk encryption of data. SHA-1 is a hashing algorithm, not an encryption algorithm.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_18]

Question 9: Correct

Which of the following is the weakest symmetric encryption method?

- (selected) DES
- Blowfish
- 3DES
- Twofish
- AES

Explanation

DES was one of the first symmetric encryption methods and is now obsolete (known weaknesses can be used to break the encryption).

3DES improves upon DES by applying the encryption three times. It is an acceptable alternative to DES. AES is stronger and faster than 3DES when implemented with a large key size (256-bits). Blowfish and Twofish were alternatives to DES, but AES was chosen to replace DES.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_19]

Question 10: Correct

What type of key or keys are used in symmetric cryptography?

- A unique key for each participant

- Two unique sets of key pairs
- A shared private key
- A single key pair

Explanation

Symmetric cryptography uses a shared private key. Both communication partners must be in possession of the same key in order to exchanged encrypted data.

Asymmetric cryptography uses a unique key pair for each participant. This key pair consists of a public key and a private key.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_12]

Question 11: Correct

What form of cryptography is best suited for bulk encryption because it is so fast?

- Asymmetric cryptography
- Hashing cryptography
- Symmetric key cryptography
- Public key cryptography

Explanation

Symmetric cryptography is best suited for bulk encryption because it is much faster than asymmetric cryptography.

Hashing is not used for encryption; it is only used to verify the integrity of data. Public key cryptography, also known as asymmetric cryptography, is best suited for small amounts of data. Often, asymmetric cryptography is used to exchange symmetric cryptography keys, and then the symmetric cryptography keys are used to encrypt communication traffic.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_13]

Question 12: Correct

How many keys are used with symmetric key cryptography?

- One
- Two
- Four
- Five

Explanation

Private key, or symmetric, cryptography uses a single *shared* key. Both communicating parties must possess the shared key to encrypt and decrypt messages. The biggest challenge to symmetric cryptography is the constant need to protect the shared private key. This protection must be applied at all times, including during the initial transmission of the shared key between the parties.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_14]

Question 13: Correct

Which of the following can be classified as a stream cipher?

- (selected) RC4
- AES
- Twofish
- Blowfish

Explanation

The most frequently used implementation of symmetric key stream ciphers is Ron's code (or Ron's cipher) v4, known as RC4. RC4 uses a variable key up to 256 bits and is commonly used with WEP and SSL. It uses the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA).

Blowfish, Twofish, and AES are all block ciphers.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_17]

Question 14: Correct

Which of the following is considered an out-of-band distribution method for private key encryption?

- Using a private fiber network
- Sending a secured email
- Using a key distribution algorithm
- (selected) Copying the key to a USB drive

Explanation

Out-of-band distribution involves manually distributing the key (for example, as copying the key to a USB drive and sending it to the other party).

Sending an email, using a key distribution algorithm, or using a private fiber network are all considered in-band distribution methods.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_22]

Question 15: Correct

Match the symmetric key distribution mechanism on the left with the appropriate description on the right. Each distribution mechanism may be used once, more than once, or not at all.

The sender's key is sent to a recipient using a Diffie-Hellman key exchange.

✓ In-band distribution

The sender's key is copied to a USB drive and handed to the recipient.

✓ Out-of-band distribution

The sender's key is sent to the recipient using public key cryptography.

✔ In-band distribution

The sender's key is burned to a CD and handed to the recipient.

✔ Out-of-band distribution

Explanation

Before communications can begin using symmetric encryption, both parties must exchange the shared secret key using a secure channel. Symmetric key encryption can use the following key distribution methods:

- *Out-of-band distribution* involves manually distributing the key, such as copying the key to a USB drive and sending it to the other party.
- *In-band distribution* can use a key distribution algorithm, such as Diffie-Hellman, to send the key to the recipient. It can also use asymmetric encryption technology to encrypt the key for distribution.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_23]

Exam Report: 9.6.3 Practice Questions

Date: 6/21/2019 9:14:14 pm
Time Spent: 1:32

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

How many keys are used with asymmetric (public key) cryptography?

- One
- Two
- Three
- Four

Explanation

Public key (asymmetric) cryptography uses two keys: one is referred to as the public key, and the other the private key. This key pair overcomes the difficulties associated with the secure distribution of private keys. The communicating parties do not need to share secret information; only the public keys are shared. Public keys are associated with users through authentication, usually through a mutually trusted directory, such as a certificate authority. The sender transmits a confidential message using only the recipient's public key. The message can only be decrypted with the associated private key possessed solely by the recipient. Public key cryptography not only provides encryption, but is the basis for authentication technologies such as digital signatures.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_01]

Question 2: Correct

A receiver wants to verify the integrity of a message received from a sender. A hashing value is contained within the digital signature of the sender.

Which of the following must the receiver use to access the hashing value and verify the integrity of the transmission?

- Sender's private key
- Receiver's private key
- Sender's public key
- Receiver's public key

Explanation

Digital signatures are created using the sender's private key. Thus, only the sender's public key

can be used to verify and open any data encrypted with the sender's private key. The recipient's private and public keys are not involved in this type of cryptography situation. Often, the hashing value of a message is protected by the sender's private key (their digital signature). The recipient must extract the original hashing value.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_02]

Question 3: Correct

Which of the follow are characteristics of ECC? (Select two.)

- [x] Uses a finite set of values within an algebraic field
- [ ] Uses multiplication of large prime numbers
- [x] Asymmetric encryption
- [ ] Symmetric encryption

Explanation

Elliptic curve cryptography (ECC) is an approach to cryptography that uses a finite set of values within an elliptic curve (an algebraic set of numbers). ECC is an asymmetric encryption algorithm.

RSA is an asymmetric algorithm that uses the multiplication of large prime numbers for encryption.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_03]

Question 4: Correct

Which of the following algorithms are used in asymmetric encryption? (Select two.)

- [x] Diffie-Hellman
- [ ] Twofish
- [x] RSA
- [ ] AES
- [ ] Blowfish

Explanation

RSA and Diffie-Hellman are asymmetric algorithms. RSA, one of the earliest encryption algorithms, can also be used for digital signatures. The Diffie-Hellman protocol was created in 1976, but is still in use today in technologies such as SSL, SSH, and IPsec.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_04]

Question 5: Correct

Which form of asymmetric cryptography is based upon Diffie-Hellman?

- ( ) Merkle-Hellman Knapsack

- RSA
- ECC
- El Gamal

Explanation

El Gamal is based upon Diffie-Hellman.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_10]

Question 6: Correct

Which cryptography system generates encryption keys that could be used with DES, AES, IDEA, RC5, or any other symmetric cryptography solution?

- Merkle-Hellman Knapsack
- RSA
- Elliptical Curve
- Diffie-Hellman

Explanation

Diffie-Hellman is the only key generation system in this list of options. Diffie-Hellman produces a number that can be used as a key in any symmetric cryptography solution (assuming the number is within the algorithm's keyspace).

Merkle-Hellman Knapsack is not a key generation system. Instead, it is an insecure concept that pre-dates public key encryption. Elliptical curve is not a key generation system. Instead, it is a method of applying other systems to gain greater strength from smaller keys. RSA is not a key generation system. Instead, it is an asymmetric cryptography system that can be used for encryption, key exchange, and digital signatures.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_11]

Question 7: Correct

Match each public key cryptography key management mechanism on the left with the corresponding description on the right. Each mechanism may be used once, more than once, or not at all.

Implements the Diffie-Hellman key exchange protocol using elliptic curve cryptography

- ✓ ECDH

Exist only for the lifetime of a specific communication session

- ✓ Ephemeral keys

Uses no deterministic algorithm when generating public keys

- ✓ Perfect forward secrecy

Can be reused by multiple communication sessions

- ✓ Static keys

Explanation

Public key cryptography can use a variety of mechanisms to manage encryption keys, including the following:

- *Ephemeral keys* are generated every time the key establishment process is executed and only exist for the lifetime of a specific communication session. As such, these keys have a relatively short lifespan.
- *Static keys* can be reused by multiple communication sessions. As such, these keys remain in use for a relatively long period of time.
- *Perfect forward secrecy* can be implemented in public key cryptography system so that random public keys are generated for each session. No deterministic algorithm is used when generating the public keys.
- *Elliptic curve Diffie-Hellman* (ECDH) is an implementation of the Diffie-Hellman key exchange protocol using elliptic curve cryptography. It allows two parties, each having their own elliptic curve public/private key pair, to generate symmetric keys simultaneously over a non-secure channel.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_12]

Question 8: Correct

Above all else, what must be protected to maintain the security and benefit of an asymmetric cryptographic solution, especially if it is widely used for digital certificates?

- (selected) Private keys
- Hash values
- Cryptographic algorithm
- Public keys

Explanation

The strength of an asymmetric cryptographic system lies in the secrecy and security of its private keys. A digital certificate and a digital signature are little more than unique applications of a private key. If the private keys are compromised for a single user, for a secured network, or for a digital certificate authority, the entire realm of trust is destroyed.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_05]

Question 9: Correct

Which of the following is used in conjunction with a local security authority to generate the private and public key pair used in asymmetric cryptography?

- (selected) CSP
- CRL
- CPS
- OCSP
- CA

Explanation

A cryptographic service provider (CSP) resides on the client and generates the key pair. This is a software program that can generate keys using a specific algorithm.

The certificate authority (CA) is an entity trusted to issue, store, and revoke digital certificates. The certificate practice statement (CPS) is a declaration of the security that the organization is implementing for all certificates issued by the CA holding the CPS.

The certificate revocation list (CRL) resides in the CA and consists of a list of certificates that have been previously revoked. The online certificate status protocol (OCSP) is a protocol used for checking the status of an individual digital certificate to verify whether it is good or has been revoked.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_06]

Question 10: Correct

Mary wants to send a message to Sam so that only Sam can read it. Which key would be used to encrypt the message?

- Mary's public key
- Sam's private key
- Sam's public key

Explanation

Use Sam's public key to encrypt the message. Only the corresponding private key, which only Sam has, can be used to decrypt the message.

Mary cannot use Sam's private key because only Sam has that key. Anything encrypted with the private key can be decrypted by anyone with the public key. Encrypting using Mary's private key would mean that anyone could read the data using Mary's public key. Encrypting with Mary's public key would mean that only Mary would be able to decrypt it using her private key.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_07]

Question 11: Correct

Mary wants to send a message to Sam. She wants to digitally sign the message to prove that she sent it. Which key would Mary use to create the digital signature?

- Mary's private key
- Sam's private key
- Sam's public key
- Mary's public key

Explanation

Use Mary's private key to create the digital signature. This proves that only Mary could have sent the message because only Mary has access to her private key. Sam would use Mary's public key to verify the digital signature.

Use Sam's public key to encrypt a message that only Sam should be able to read. Only the corresponding private key, which only Sam has, can be used to decrypt the message.

Mary cannot use Sam's private key because only Sam has that key. Anything encrypted with the private key can be decrypted by anyone with the public key. Encrypting with Mary's public

key would mean that only Mary would be able to decrypt it using her private key, but could not prove where the message came from because anyone has access to Mary's public key.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_08]

Question 12: Correct

The success of asymmetric encryption is dependent upon which of the following?

- The complexity of the cipher text
- The secrecy of the algorithm
- The secrecy of the key
- The integrity of the individuals who created the cryptosystem

Explanation

The strength of an asymmetric encryption system lies in the secrecy and security of its private keys. The strength of a cryptosystem should not be in the secrecy of the algorithm. This means that the algorithm is usually published and can be scrutinized for weaknesses.

References

LabSim for Security Pro, Section 9.6.
[All Questions SecPro2017_v6.exm ASYM_ENCRYPT_09]

Exam Report: 9.7.10 Practice Questions

Date: 6/24/2019 10:45:16 am
Time Spent: 0:48

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 88%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You would like to implement BitLocker to encrypt data on a hard disk, even if it is moved to another system. You want the system to boot automatically without providing a startup key on an external USB device.

What should you do?

- Enable the TPM in the BIOS
- Disable USB devices in the BIOS
- Use a PIN instead of a startup key
- Save the startup key to the boot partition

Explanation

When a system boots, the startup key is required to unlock the encrypted volume. The system startup key can be saved in the Trusted Platform Module (TPM). With the startup key saved in the TPM, the system can start without additional intervention.

The system will not start without the startup key. Without a TPM, the startup key must be stored on a USB drive. You can require a PIN in addition to a startup key, but the PIN cannot replace the startup key. Storing the startup key on the boot drive would expose it to compromise.

References

LabSim for Security Pro, Section 9.7.
[All Questions SecPro2017_v6.exm FILE_ENCRYPT_01]

Question 2: Correct

You want to protect data on hard drives for users with laptops. You want the drive to be encrypted, and you want to prevent the laptops from booting unless a special USB drive is inserted. In addition, the system should not boot if a change is detected in any of the boot files.

What should you do?

- Have each user encrypt user files with EFS.
- Implement BitLocker without a TPM.
- Have each user encrypt the entire volume with EFS.
- Implement BitLocker with a TPM.

Explanation

Use BitLocker to encrypt the entire system volume and protect both operating system and user data. Use BitLocker with a Trusted Platform Module (TPM) to protect the boot environment components such as the BIOS, Master Boot Record, Boot Sector, Boot Manager, and Windows Loader. The system is shut down if a boot environment change is detected. Using BitLocker, drives are locked if they are moved to another computer, and you can require a startup key on a USB drive or a PIN before the system will boot.

If you use BitLocker without a TPM, system integrity checks are not performed. The TPM is required for saving the startup file information that is used to verify system integrity. When using BitLocker without a TPM, you must use a startup key on a USB device; when using a TPM, this is an optional configuration.

EFS encrypts individual files. With EFS, only the user who encrypted the file and any additionally designated users can access the file. EFS does not provide integrity checks for boot files.

References

LabSim for Security Pro, Section 9.7.
[All Questions SecPro2017_v6.exm FILE_ENCRYPT_02]

Question 3: Correct

Which of the following security measures encrypts the entire contents of a hard drive?

- BIOS password
- Chassis intrusion detection
- Trusted Platform Module (TPM)
- DriveLock
- Hard disk password

Explanation

DriveLock encrypts the entire contents of a hard drive, protecting all files on the disk.

When a password is set for the hard drive, you cannot move the drive to another system to access the disk without the password (the password moves with the disk). A Trusted Platform Module (TPM) is a special chip on the motherboard that generates and stores cryptographic keys to verify that the hardware has not changed. This value can be used to prevent the system from booting if the hardware has changed. Chassis intrusion detection helps you identify when a system case has been opened. When the case cover is removed, the switch sends a signal to the BIOS. A BIOS password controls access to the system. If set, the administrator (or supervisor or setup) password is required to enter the CMOS program to make changes to BIOS settings.

References

LabSim for Security Pro, Section 9.7.
[All Questions SecPro2017_v6.exm FILE_ENCRYPT_03]

Question 4: Correct

You want a security solution that protects the entire hard drive and prevents access even if the drive is moved to another system. Which solution should you choose?

- EFS
- IPsec
- BitLocker

- VPN

Explanation

BitLocker is a Microsoft security solution that encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key that is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer.

EFS is a Windows file encryption option, but only encrypts individual files. Encryption and decryption is automatic and dependent upon the file's creator and whether other uses have read permissions.

A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

References

LabSim for Security Pro, Section 9.7.
[All Questions SecPro2017_v6.exm FILE_ENCRYPT_04]

Question 5: Incorrect

You've used BitLocker to implement full volume encryption on a notebook system. The notebook motherboard does not have a TPM chip, so you've used an external USB flash drive to store the BitLocker startup key.

Which system components are encrypted in this scenario? (Select two.)

- [ ] System partition
- [ ] Optical media
- [x] Master boot record
- [ ] BIOS
- [ ] C:\ volume

Explanation

BitLocker uses full volume encryption, so the disk partition containing the C:\ volume is encrypted along with the master boot record.

However, BitLocker does not encrypt the 100 MB system partition that contains the boot files, nor the system BIOS or RAM.

References

LabSim for Security Pro, Section 9.7.
[All Questions SecPro2017_v6.exm FILE_ENCRYPT_06]

Question 6: Correct

You've used BitLocker to implement full volume encryption on a notebook system. The notebook motherboard does not have a TPM chip, so you've used an external USB flash drive to store the BitLocker startup key.

You use EFS to encrypt the C:\Secrets folder and its contents.

Which of the following is true in this scenario? (Select two.)

- [ ] Any user who is able to boot the computer from the encrypted hard disk will be able to open the C:\Secrets\confidential.docx file.
- [ ] If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, it will remain in an encrypted state.

- [ ] The EFS encryption process will fail.
- [ ] Only the user who encrypted the C:\Secrets\confidential.docx file will be able to boot the computer from the encrypted hard disk.
- [x] By default, only the user who encrypted the C:\Secrets\confidential.docx file will be able to open it.
- [x] If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, it will be saved in an unencrypted state.

Explanation

BitLocker uses full volume encryption, while EFS is used to encrypt individual files and folders. The following are true in this scenario:

- If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, it will be saved in an unencrypted state.
- Only the user who encrypted the C:\Secrets\confidential.docx file will be able to open it by default.

With BitLocker enabled, any user who has the appropriate startup key or PIN is able to boot the system from the encrypted drive. However, only the user who encrypted the C:\Secrets\ folder will be able to access files within it unless additional user accounts are explicitly added.

References

LabSim for Security Pro, Section 9.7.
[All Questions SecPro2017_v6.exm FILE_ENCRYPT_07]

Question 7: Correct

Which of the following security solutions would prevent a user from reading a file that she did not create?

- (●) EFS
- ( ) BitLocker
- ( ) IPsec
- ( ) VPN

Explanation

EFS is a Windows file encryption option that encrypts individual files so that only the user who created the file can open it. Decryption is automatic when the file owner opens it. Other users cannot open the encrypted file unless specifically authorized.

BitLocker is a Microsoft security solution that encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key that is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer. A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

References

LabSim for Security Pro, Section 9.7.
[All Questions SecPro2017_v6.exm FILE_ENCRYPT_05]

Question 8: Correct

You create a new document and save it to a hard drive on a file server on your company's network. Then you employ an encryption tool to encrypt the file using AES. This activity is an

example of accomplishing which security goal?

- Integrity
- Confidentiality
- Non-repudiation
- Availability

Explanation

Encrypting a file while it is stored on a hard drive is usually done to provide protection for the object's confidentiality.

Hashing is used to provide integrity. Using mechanisms like backups and avoiding single points of failure provide availability protection. Non-repudiation is usually provided for during a secured communication, not usually while a file is stored on a hard drive.

References

LabSim for Security Pro, Section 9.7.
[All Questions SecPro2017_v6.exm FILE_ENCRYPT_08]

Exam Report: 9.8.8 Practice Questions

Date: 6/24/2019 10:59:53 am
Time Spent: 1:19

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 93%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which aspect of a certificate makes it a reliable and useful mechanism for proving the identity of a person, system, or service on the internet?

- It uses electronic signatures.
- It is a digital mechanism, rather than a physical one.
- It is a trusted third-party.
- It provides ease of use.

Explanation

The use of a trusted third-party (called a Certificate Authority or CA) is what makes certificates a reliable and useful mechanism for proving the identity of a person, system, or service on the internet. The CA issues proof of identity to each organization in the form of a certificate. The fact that all entities trust the CA makes the certificates trusted and valuable.

A certificate only proves identity; it does not prove reliability. Electronic signatures are a form of certificate that verifies identity. While electronic signatures prove identity, they do so only because both parties trust the authority of the CA, not because the signature exists. Certificates are easy to use. However, ease of use does not make them reliable. Certificates are a digital mechanism, which makes them suited for use on the internet. However, that alone does not make them reliable or useful.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_02]

Question 2: Incorrect

Which standard is most widely used for certificates?

- X.509
- 802.1x
- ~~SSL v.3.0~~
- HTTP 1.1

Explanation

The standard for certificates that is most widely used is X.509. This standard defines the key elements that must exist within a certificate. This standard is used by PKI (Public Key

Infrastructure), SSL, IPsec, DES, and many other infrastructure components and technologies. HTTP 1.1 is the latest version of the protocol used to transmit web resources from a web server to a web client. SSL v.3.0 uses certificates, but this is the standard for the secure session protocol for protecting web communications. 802.1x is a networking protocol that defines how to support EAP (Extensible Authentication Protocol) over a wired or wireless LAN.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_04]

Question 3: Correct

Which of the following items are contained in a digital certificate? (Select two.)

- [x] Public key
- [x] Validity period
- [ ] Private key
- [ ] Root CA secret key

Explanation

Digital certificates create a link between identities and public keys. A certificate contains the information necessary to identify the public key owner. Certificates include fields detailing the issuing CA and the standards version used to generate the certificate, a certificate serial number, all approved uses for the certificate, the certificate owner, the public key and algorithm, the validity period, and the algorithms used to digitally sign the certificate. Additional functionality and data may be added through the use of certificate extensions.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_06]

Question 4: Correct

Which of the following conditions does **not** result in a certificate being added to the certificate revocation list?

- ( ) Invalid identity credentials
- ( ) Private key compromise
- ( ) Committing a crime using the certificate
- (•) Certificate expiration

Explanation

When a certificate's valid time value expires, the certificate immediately becomes invalid because it has expired. Expired certificates are not added to the CRL because the timestamp serves as notification that the certificate is no longer valid.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_08]

Question 5: Correct

Which of the following is an entity that accepts and validates information contained within a request for a certificate?

- Recovery agent
- ➡ Registration authority
- Certificate authority
- Enrollment agent

Explanation

A Registration Authority (RA) can be used in large enterprise environments to offload client enrollment request processing by handling client verification prior to certificates issue. The RA accepts registrations, validates identity, and approves or denies certificate requests.

The Certificate Authority (CA) is an entity trusted to issue, store, and revoke digital certificates. Often, the role of CA is combined with that of RA. But technically speaking, a CA is the computer that issues the certificate. *Recovery agents* are users who are given the ability to restore private keys from the archive. An enrollment agent is someone who can request a certificate on behalf of another user. Enrollment agents are often used to request certificates used on smart cards.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_10]

Question 6: Correct

What is a PKI?

- A protocol that defines secure key exchange.
- ➡ A hierarchy of computers for issuing certificates.
- An algorithm for encrypting and decrypting data.
- A program that generates key pairs.

Explanation

A public key infrastructure (PKI) is a hierarchy of computers that issue and manage certificates.

A Cryptographic Service Provider (CSP) resides on the client and generates the key pair. Secure exchange of keys is provided by many protocols, including RSA, Diffie-Hellman, IKE, and KEA.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_12]

Question 7: Correct

A PKI is an implementation for managing which type of encryption?

- ➡ Asymmetric
- Steganography
- Hashing
- Symmetric

Explanation

A public key infrastructure (PKI) is a hierarchy of computers that issue and manage certificates. Certificates use asymmetric encryption with a public and a private key pair.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_14]

Question 8: Correct

Certificate revocation should occur under all but which of the following conditions?

- The certificate owner has committed a crime while using the certificate
- The certificate owner has moved their website to a new domain name
- The certificate owner has changed their business name
- The certificate owner has held the certificate beyond the established lifetime timer

Explanation

A certificate does not need to be revoked once it expires. The possession of an expired certificate is useless.

A certificate should be revoked whenever the owner commits a crime using the certificate or when a significant aspect of the identity of the organization changes.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_16]

Question 9: Correct

Which technology was developed to help improve the efficiency and reliability of checking the validity status of certificates in large, complex environments?

- Private Key Recovery
- Key Escrow
- Certificate Revocation List
- Online Certificate Status Protocol

Explanation

Online Certificate Status Protocol (OCSP) is the technology developed to improve the efficiency and reliability of checking the validity status of certificates in large complex environments. OCSP allows clients to query a CA or registration authority (RA) and quickly learn whether a certificate is valid or has been revoked.

OCSP is a significant improvement over the CRL mechanism. CRLs were static lists that were distributed periodically to CAs and RAs. However, CRLs were often out of date. Key escrow and private key recovery are not related to certificate status checking.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_18]

Question 10: Correct

Which action is taken when the private key associated with a digital certificate becomes compromised?

- All certificates are revoked from parties known to possess the matching public key.

The certificate is revoked and added to the Certificate Revocation List.

- The CA retracts all previously issued copies of the certificate.
- The RA requests a reissued digital signature based on the existing private key.

Explanation

When a private key becomes compromised, the certificate authority revokes the certificate and adds it to the certificate revocation list (CRL). This list notifies anyone attempting to verify the digital signature that the certificate is not trustworthy. The CRL is designed to prevent impersonation by anyone obtaining unauthorized access to a private key.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_20]

Question 11: Correct

You have lost the private key that you have used to encrypt files. You need to get a copy of the private key to open some encrypted files. Who should you contact?

- Registration Authority
- Recovery agent
- Enrollment agent
- Certification Authority

Explanation

Recovery agents are users who are given the ability to restore private keys from the archive. An enrollment agent is someone who can request a certificate on behalf of another user.

Enrollment agents are often used to request certificates used on smart cards.

A Registration Authority (RA) can be used in large enterprise environments to offload client enrollment request processing by handling client verification prior to certificate issue. The RA accepts registrations, validates identity, and approves or denies certificate requests.

The Certificate Authority (CA) is an entity trusted to issue, store, and revoke digital certificates. Often, the role of CA is combined with that of RA. But technically speaking, the CA is the computer that issues the certificate.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_22]

Question 12: Correct

To obtain a digital certificate and participate in a Public Key Infrastructure (PKI), what must be submitted and where?

- Identifying data with the MAC and IP addresses to the root certificate authority (CA)
- Identifying data and a secret key request to the subordinate distribution authority (DA)
- Identifying data with the 3DES block cipher to the hosting certificate authority (CA)
- Identifying data and a certification request to the registration authority (RA)

Explanation

The registration authority (RA) processes all requests for digital certificates. Registration and authentication requirements vary based on the class of certificate requested. Once the RA has

successfully authenticated the requesting party, the request is forwarded to the certificate authority (CA) for certificate generation.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_24]

Question 13: Correct

An SSL client has determined that the Certificate Authority (CA) issuing a server's certificate is on its list of trusted CAs. What is the next step in verifying the server's identity?

- ○ The domain on the server certificate must match the CA's domain name.
- ○ The master secret is generated from common key code.
- ➡ ◉ The CA's public key must validate the CA's digital signature on the server certificate.
- ○ The post-master secret must initiate subsequent communication.

Explanation

Once an SSL client has identified a CA as trusted, it uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.

SSL clients verify a server's identity with the following steps:

1. The client checks the server's certificate validity period. The authentication process stops if the current date and time fall outside of the validity period.
2. The client verifies that the issuing Certificate Authority (CA) is on its list of trusted CAs.
3. The client uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.
4. To protect against Man-in-the-Middle attacks, the client compares the actual DNS name of the server to the DNS name on the certificate.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_26]

Question 14: Correct

How many keys are used with Public Key cryptography?

- ○ One
- ➡ ◉ Two
- ○ Three
- ○ Four

Explanation

Public Key cryptography uses two keys: one is referred to as the public key, and the other, the private key. This key pair overcomes the difficulties associated with the secure distribution of private keys. The communicating parties do not need to share secret information: only the public keys are shared. Public keys are associated with users through authentication, usually through a mutually trusted directory, such as a certificate authority. The sender transmits a confidential message using only the recipient's public key. The message can only be decrypted with the associated private key possessed solely by the recipient. Public Key cryptography not only provides encryption, but is the basis for authentication technologies such as digital signatures.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_27]

Question 15: Correct

When is the best time to apply for a certificate renewal?

- After a certificate has been revoked
- Just after a certificate expires
- Immediately after a certificate is issued
- Near the end of the certificate's valid lifetime

Explanation

Certificate renewal is a process by which a currently valid certificate is re-issued with an extended lifetime value. It is performed by submitting a renewal request and signing the request with the still-valid certificate.

Attempting to renew a certificate close to its issuance date will not result in a renewal in most cases. There is no need to renew a certificate until you near the end of its valid lifetime. It is not possible to renew a certificate after it has expired or been revoked; these conditions require you to request a new certificate.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_30]

Exam Report: 9.9.5 Practice Questions

Date: 6/24/2019 11:08:59 am
Time Spent: 0:50

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Hashing algorithms are used to perform what activity?

- Provide a means for exchanging small amounts of data securely over a public network
- Create a message digest
- Encrypt bulk data for communications exchange
- Provide for non-repudiation

Explanation

Hashing algorithms are used to create a message digest to ensure that data integrity is maintained. A sender creates a message digest by performing the hash function on the data files that will be transmitted. The receiver performs the same action on the data received and compares the two message digests. If they are the same, then the data was not altered.

Symmetric algorithms are used to encrypt bulk data for communications exchange. Asymmetric algorithms provide a means for exchanging small amounts of data securely over a public network. Both symmetric and asymmetric algorithms provide for non-repudiation.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_01]

Question 2: Correct

Which of the following best describes high amplification when applied to hashing algorithms?

- Dissimilar messages frequently result in the same hash value.
- A small change in the message results in a big change in the hash value.
- Hashes produced by two different parties using the same algorithm result in the same hash value.
- Reversing the hashing function does not recover the original message.

Explanation

High amplification, also known as the *avalanche effect*, means that a small change in the message results in a big change in the hashed value.

Hashes are one-way functions, meaning that once you hash a message, you cannot reverse the hashing algorithm to extract the data. Data integrity is proven when the same hashing

algorithm performed on a message results in the same hash value. A *collision* results when two different messages produce the same hash value (a low number of collisions is desirable).

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_02]

Question 3: Correct

Which of the following is the strongest hashing algorithm?

- MD5
- NTLM
- LANMAN
- SHA-1

Explanation

SHA-1 is the strongest hashing algorithm. SHA-1 generates a message digest of 160 bits.

MD-5 is weaker than SHA-1, producing a message digest of 128 bits. LANMAN and NTLM both use hashing to protect authentication credentials, but these protocols are not used for creating hashes of data. LANMAN is less secure than NTLM, with either method being less secure than MD-5 (NTLM uses either MD-4 or MD-5 to produce the hash).

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_06]

Question 4: Correct

Which of the following is the weakest hashing algorithm?

- SHA-1
- DES
- MD5
- AES

Explanation

MD5 is the weakest hashing algorithm. It produces a message digest of 128 bits. The larger the message digest, the more secure the hash. SHA-1 is more secure because it produces a 160-bit message digest.

Both DES and AES are symmetric encryption algorithms. DES is weaker than AES.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_07]

Question 5: Correct

SHA-1 uses which of the following bit length hashing algorithms?

- Only 160-bit
- 224-bit, 256-bit, 384-bit, and 512-bit
- Only 128-bit

- 128-bit, 160-bit, 192-bit, 224-bit, and 256-bit

Explanation

SHA-1 is a 160-bit hashing algorithm. It is capable of producing 2160 different combinations.

MD-2 and MD-4 are both 128-bit hashing algorithms. HAVAL is a 128-bit, 160-bit, 192-bit, 224-bit, and 256- bit hashing algorithm. SHA-2, a newer version of SHA-1, is a 224-bit, 256-bit, 384-bit, 512-bit hashing algorithm.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_08]

Question 6: Correct

Which of the following does not or cannot produce a hash value of 128 bits?

- RIPEMD
- MD2
- SHA-1
- MD5

Explanation

SHA-1 produces hash values of 160 bits.

MD5 and MD2 both produce hash values of 128 bits. Haval can produce 128-bit hash values because it can produce a hash value of any length.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_09]

Question 7: Correct

A birthday attack focuses on what?

- E-commerce
- Encrypted files
- VPN links
- Hashing algorithms

Explanation

A birthday attack focuses on hashing algorithms. Birthday attacks exploit the probability that two messages using the same hash algorithm will produce the same message digest. This is also known as exploiting collision. If two different messages or files produce the same hashing digest, then a collision has occurred.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_10]

Question 8: Correct

When two different messages produce the same hash value, what has occurred?

- Hash value

- Collision
- High amplification
- Birthday attack

Explanation

A *collision* occurs when two different messages produce the same hash value.

A birthday attack is a brute force attack in which the attacker hashes messages until one with the same hash is found. A hash value is the result of a compressed and transformed message (or some type of data) into a fixed-length value. High amplification means a small change in the message results in a big change in the hashed value.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_03]

Question 9: Correct

Which of the following is used to verify that a downloaded file has not been altered?

- Symmetric encryption
- Asymmetric encryption
- Hash
- Private key

Explanation

A *hash* is a function that takes a variable-length string (message) and compresses and transforms it into a fixed-length value. Hashes ensure the data integrity of files and messages in transit. For example, when users post files for download, they often create a hash value for the file. After you download the file, you can create a hash using the same algorithm. If the hash values match, you know that the file you have matches the original file.

Symmetric encryption is typically used for fast data encryption. Asymmetric encryption is used for encrypting small amounts of data or exchanging keys used with symmetric encryption. A private key is one of the keys used in asymmetric encryption.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_04]

Question 10: Correct

You have just downloaded a file. You create a hash of the file and compare it to the hash posted on the website. The two hashes match.

What do you know about the file?

- No one has read the file contents as it was downloaded.
- You will be the only one able to open the downloaded file.
- You can prove the source of the file.
- Your copy is the same as the copy posted on the website.

Explanation

A *hash* is a function that takes a variable-length string (message) and compresses and transforms it into a fixed-length value. Hashes ensure the data integrity of files and messages in transit. The sender and the receiver use the same hashing algorithm on the original data. If the hashes match, then it is assumed that the data is unmodified.

Hashes do not ensure confidentiality (in other words, hashes are not used to encrypt data). Non-repudiation proves the source of a file and is accomplished using digital signatures.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_05]

Exam Report: 9.11.3 Practice Questions

Date: 6/24/2019 2:57:00 pm
Time Spent: 1:23

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following DLP implementations can be used to monitor and control access to the physical devices on workstations or servers?

- Network DLP
- ➡ Endpoint DLP
- Cloud DLP
- File-level DLP

Explanation

Endpoint DLP runs on end user workstations and servers. Endpoint DLP is also referred to as a Chinese Wall solution. It could be something as simple as restricting the use of USB devices. Many endpoint-based systems also provide application controls to prevent confidential information transmission. They also provide some type of immediate feedback to the user. Giving feedback to the user is based on the concept that not all data leakage incidents are malicious. The employee might not realize that the security policy violation notification is appropriate. The intent is to deter the employee from a similar action in the future.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_05]

Question 2: Correct

DLP can be implemented as a software or hardware solution that analyzes traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.

Which of the following DLP implementations analyzes traffic for data containing such things as financial documents, social security numbers, or key words used in proprietary intellectual property?

- ➡ Network DLP
- Cloud DLP
- File-level DLP
- Endpoint DLP

Explanation

Network DLP is a software or hardware solution that is typically installed near the network

perimeter. It analyzes network traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_03]

Question 3: Correct

Which of the following is a technology that tries to detect and stop sensitive data breaches, or data leakage incidents, in an organization?

- Data transmission security
- Data hashing
- Data loss prevention
- Public key cryptography

Explanation

Data loss prevention (DLP) is a technology that tries to detect and stop sensitive data breaches, or data leakage incidents, in an organization. DLP is used to prevent sensitive data from being disclosed to an unauthorized person, whether it is deliberate or accidental.

Data transmission security is the use of secure protocols to encrypt data when it is transmitted. Hashing takes a variable-length string (message) and compresses and transforms it into a fixed-length value. When received, the hash is decrypted into the actual output so the recipient can understand the message. Public key infrastructure uses certificates, which are electronic document that uses a digital signature, to bind a public key with an identity.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_01]

Question 4: Correct

DLP can be used to identify sensitive files in a file system and then embed the organization's security policy within the file.

Which of the following DLP implementations travels with sensitive data files when they are moved or copied?

- Endpoint DLP
- Network DLP
- File-level DLP
- Cloud DLP

Explanation

File-Level DLP is used to identify sensitive files in a file system and then to embed the organization's security policy within the file so that it travels with the file when it is moved or copied. Since the security policy travels with that file if it's moved or copied, you can continue to control access to the file, such as restricting who it can be transmitted to, even when the file is no longer on your system.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_04]

Question 5: Correct

Sensitive data is monitored by the data loss prevention (DLP) system in four different states. Which of the following is NOT one of the states monitored by DLP?

- While being transmitted to or from cloud-based systems.
- While in motion as it is transmitted over the network.
- While at rest on a storage medium.
- ➡ While a file with sensitive data is being created.
- While in use on endpoint systems.

Explanation

DLP does not monitor sensitive data while files are being created.

Sensitive data is monitored by the DLP system in four different states:

- While in use on endpoint systems to monitor and control access to physical devices on workstations or servers.
- While in motion as it is transmitted over the network.
- While at rest on a storage medium.
- While being transmitted to or from cloud-based systems.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_02]

Exam Report: 9.12.10 Practice Questions

Date: 6/24/2019 5:31:30 pm
Time Spent: 1:58

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What is the primary security feature that can be designed into a network's infrastructure to protect and support availability?

- Periodic backups
- Fiber optic cables
- Switches instead of hubs
- Redundancy

Explanation

Redundancy is the primary security feature that can be designed into a network's infrastructure to protect and support availability, since it identifies single points of failure.

Periodic backups are better than no backups, but real-time and off-site backups are better protections for availability. Fiber optic cables are not a real protection for a network's availability, as they only provide the security benefit of eavesdropping protection. Switches are better than hubs, but there are infrastructure security measures that provide more significant protections for availability.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_01]

Question 2: Correct

Which form of alternate site is the cheapest, but may not allow an organization to recover before reaching their maximum tolerable downtime?

- Warm site
- Service bureau
- Hot site
- Reciprocal agreement

Explanation

A reciprocal agreement is a contract between two organizations that states in the event of a disaster they will aid each other by sharing their IT processing capabilities. Reciprocal agreements have no initial cost related to them. However, most organizations can barely support their own IT needs, much less the needs of an entire second organization.

A hot site, warm site, and service bureau contracts are all costly alternatives, but offer reasonable if not reliable assurance of recovery in the event of a disaster.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_02]

Question 3: Correct

You manage a website for your company. The website uses three servers configured in a cluster. Incoming requests are distributed automatically between the three servers. All servers use a shared storage device that holds the website contents. Each server has a single network connection and a single power supply.

Considering the availability of your website, which component represents a single point of failure?

- Network adapter
- Power supply
- Website storage
- Web server

Explanation

In this scenario, the shared storage is a single point of failure. A single point of failure means that failure in one component will cause the entire website to be unavailable. If the storage unit fails, then the website content will be unavailable.

Failure in a single network card, power supply, or even in a single server will not make the website unavailable. Any of these failures will take one server offline. But because of the server cluster, other servers will still be available to process incoming requests.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_07]

Question 4: Correct

You manage your company's website. The Web1 server hosts the website. This server has the following configuration:

- Dual core processor
- Dual power supplies
- RAID 5 volume
- One RAID controller
- Two 1000 Mbps network adapters

Which component is a single point of failure for the website?

- Disk controller
- Disk storage
- Power supply
- Network adapter

Explanation

A single point of failure means that failure in one component will cause the entire website to be unavailable. In this scenario, the disk controller is a single point of failure. If the disk controller fails, content for the website will be unavailable.

To prevent a single point of failure, provide redundant components. Dual power supplies, multiple network connections, and fault tolerant volumes (RAID 1, RAID 5, or RAID 0 + 1) can all sustain a failure in one component and continue to function.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_08]

Question 5: Correct

Which of the following disk configurations might sustain losing two disks? (Select two.)

- [ ] RAID 1
- [x] RAID 1+0
- [x] RAID 0+1
- [ ] RAID 5

Explanation

RAID 1+0 combines disk mirroring (1) and disk striping (0). Multiple disks are configured into two mirrored arrays, which are then striped across the other set. RAID 1+0 can sustain multiple drive losses as long as no mirror loses all its drives. RAID 0+1 can also continue to work if both failed disks are in the same set; if a set in each disk fails, data is unavailable.

RAID 5 and RAID 1 can only sustain a loss of a single disk.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_09]

Question 6: Correct

You have been asked to implement a RAID 5 solution for your network. What is the minimum number of hard disks that can be used to configure RAID 5?

- ( ) 2
- (•) 3
- ( ) 4
- ( ) 5
- ( ) 6

Explanation

A RAID 5 array stripes data and parity information across multiple hard disks. To complete a RAID 5 array, a minimum of three hard disks is required.

RAID 0 and RAID 1 can both be implemented with a minimum of two hard disks.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_10]

Question 7: Correct

What option is an advantage RAID 5 has over RAID 1?

- ( ) RAID 5 provides redundancy for the disk controller.

- RAID 5 continues to operate with a failure in two disks; RAID 1 can only operate with a failure of one disk.
- RAID 5 provides redundancy; RAID 1 does not.
- RAID 5 improves performance over RAID 1.

Explanation

RAID 5 provides both fault tolerance and improved performance. RAID 1 (mirroring) provides only fault tolerance with no performance benefit.

Both RAID 5 and RAID 1 can only sustain a loss of one disk in the set. Use multiple disk controllers to provide redundancy for the disk controller.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_11]

Question 8: Correct

You have a computer with three hard disks.

- A RAID 0 volume uses space on Disk 1 and Disk 2.
- A RAID 1 volume uses space on Disk 2 and Disk 3.

Disk 2 fails. Which of the following is true?

- Data on the RAID 0 volume is accessible; data on the RAID 1 volume is not.
- Data on the RAID 1 volume is accessible; data on the RAID 0 volume is not.
- Data on both volumes is still accessible.
- Data on both volumes is not accessible.

Explanation

In this scenario, Disk 2 is shared between both volumes. If Disk 2 fails, the RAID 1 volume is still accessible because RAID 1 (mirrored) volumes can sustain the loss of a single disk. The data on the RAID 0 volume is not accessible. RAID 0 uses striping, which distributes the data evenly between multiple disks. If a single disk fails, the entire volume is lost.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_12]

Question 9: Correct

You have a web server on your network that hosts the public website for your company. You want to make sure that the website will continue to be available even if a NIC, hard drive, or other problem prevents the server from responding.

Which solution should you implement?

- QoS
- Load balancing
- NIC teaming
- Traffic shaping

Explanation

Load balancing configures a group of servers in a logical group (called a *server farm*). Incoming requests to the group are distributed to individual members within the group. Load balancing provides fault tolerance if the load balancing mechanism is able to detect when a specific farm member is unavailable, automatically distributing new requests to the available members.

With NIC teaming, two or more physical connections to the same network are logically grouped (or bonded). If one NIC fails, the second NIC with a connection to the same network can still be used. NIC teaming provides redundancy for a network adapter, but not for other components, such as hard drives.

A *traffic shaper* (also called a *bandwidth shaper*) is a device that is capable of modifying the flow of data through a network in response to network traffic conditions. Quality of Service (QoS) refers to a set of mechanisms that tries to guarantee timely delivery or minimal delay of important or time-sensitive communications. QoS is particularly important when implementing Voice over IP (VoIP), Video over IP, or online gaming where delay or data loss make the overall experience unacceptable.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_15]

Question 10: Correct

You manage a server that runs your company website. The web server has reached its capacity, and the number of client requests is greater than the server can handle.

You would like to find a solution so that a second server can respond to requests for website content.

Which solution should you implement?

- QoS
- Traffic shaper
- Ethernet bonding
- Load balancing

Explanation

Load balancing configures a group of servers in a logical group (called a *server farm*). Incoming requests to the group are distributed to individual members within the group. Incoming requests can be distributed evenly between group members or unevenly based on additional criteria, such as server capacity. The primary goal of load balancing is to improve performance by configuring multiple devices to respond as one.

A *traffic shaper* (also called a *bandwidth shaper*) is a device that is capable of modifying the flow of data through a network in response to network traffic conditions. Quality of Service (QoS) refers to a set of mechanisms that tries to guarantee timely delivery or minimal delay of important or time-sensitive communications. QoS is particularly important when implementing Voice over IP (VoIP), Video over IP, or online gaming--programs in which delay or data loss make the overall experience unacceptable.

With Ethernet *bonding* (also called NIC *teaming*), two or more physical connections to the same network are logically grouped (or bonded). Data is divided and sent on multiple interfaces, effectively increasing the speed at which the device can send and receive on the network.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_16]

Question 11: Correct

To prevent server downtime, which of the following components should be installed redundantly in a server system?

- Floppy disk drive
- CD or DVD drive
- RAM modules
- Power supply

Explanation

To prevent server downtime, you should install redundant power supplies in a server system. If one fails, the other can immediately take over, allowing the server to remain running.

Because it isn't a critical component, a redundant CD or DVD drive probably isn't necessary. Unless data was shared from a disc in the drive, a failed CD or DVD drive probably won't affect the server's functionality. With most motherboards, there's no way to install redundant RAM modules. Like CD or DVD drives, the floppy disk drive isn't a critical component. A failed floppy disk drive won't bring the server down.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_19]

Question 12: Correct

Match the recovery term on the right with the appropriate definition on the left.

MTTF

- Measures the average time to failure of a system or component.

MTD

- Identifies the length of time an organization can survive with a specified service, asset, or process down.

MTTR

- Identifies the average amount of time necessary to repair a failed component or to restore operations.

MTBF

- Identifies the average lifetime of a system or component.

Explanation

Redundancy measurement parameters include the following:

- *Mean Time Between Failures* (MTBF) identifies the average lifetime of a system or component. Components should be replaced around the time that the MTBF is reached.
- *Mean Time To Failure* (MTTF) measures the average time to failure of a system or component. This metric assumes that the system or component is not repaired at any point in its lifetime, which would extend its useful life.
- *Mean Time To Repair* (MTTR) identifies the average amount of time to repair a failed component or restore operations. This is also referred to as Mean Time to Restore.
- *Maximum Tolerable Downtime* (MTD) combines the RPO, RTO, MTBF, and MTTR to identify the length of time an organization can survive with a specified service, asset, or process down.

References

LabSim for Security Pro, Section 9.12.

[All Questions SecPro2017_v6.exm REDUNDANCY_21]

Question 13: Correct

You have been asked to deploy a network solution that includes an alternate location where operational recovery is provided within minutes of a disaster. Which of the following strategies would you choose?

- (selected) Hot site
- Hot spare
- Cold site
- Warm site
- HSTG

Explanation

A hot site is a complete disaster recovery facility that could be fully operational within hours or minutes in the event of a disaster. This includes maintaining redundant hardware and up-to-date network data.

A warm site is a remote network location that maintains a backup of the data, but it is not always current. Data may be days or weeks old, depending on backup procedures. A cold site provides a space and sometimes hardware in an alternate location that can be configured when needed. Returning to an operational state may take days. A hot spare is a redundant hardware component used as a failover solution.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_05]

Question 14: Correct

If your mission-critical services have a maximum tolerable downtime (MTD) (or a recovery time objective [RTO]) of 36 hours, what is the optimum form of recovery site?

- Cold
- Hot
- (selected) Warm
- Mobile

Explanation

A warm site would be the most optimum. A warm site can often provide recovery within the stated time period, and it has the most reasonable cost for the situation.

With an MTD/RTO of 36 hours, a cold site is out of the question because recovery would take much longer than the allotted time. Obviously, a hot site would offer instant recovery, but at a significant financial, administrative, management, and security cost. Nothing about the scenario indicates that a mobile backup is needed or preferred.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_17]

Question 15: Correct

Which of the following is a recovery site that may have electricity connected, but there are no servers installed and no high-speed data lines present?

- Warm site
- Hot site
- Reciprocal agreement
- Cold site

Explanation

A *cold site* is a recovery site that may have electricity connected, but there are no servers installed and no high-speed data lines present. A cold site does not offer an adequate route to recovery for most organizations.

A *hot site* is a real-time full mirror of the primary site. It is fully functional and ready for immediate use 24/7. A *warm site* is partially configured and may require days or weeks to bring up to production level. A *reciprocal agreement* is not a form of recovery site; instead, it is a non-enforceable agreement between two companies to assist each other in the event of a disaster.

References

LabSim for Security Pro, Section 9.12.
[All Questions SecPro2017_v6.exm REDUNDANCY_18]

Exam Report: 9.13.10 Practice Questions

Date: 6/25/2019 8:49:08 pm
Time Spent: 1:09

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Even if you perform regular backups, what must be done to ensure that you are protected against data loss?

- Store the backup media in an onsite fireproof vault
- Regularly test restoration procedures
- Write-protect all backup media
- Restrict restoration privileges to system administrators

Explanation

The only way to ensure that you have protection against data loss is to regularly test your restoration procedures. This activity will reveal whether or not your backup process is functioning properly and whether or not your restoration and recovery procedures are accurate.

It is a good idea to store backup media in a fireproof vault, but it is a better idea to store it offsite. Restoration privileges should be restricted to trusted staff to prevent confidentiality violations. However, this does not address the issue of data-loss protection. Write-protecting backup media provides little real security for the stored data because anyone can flip the switch on the media to remove the protection.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_01]

Question 2: Correct

When should a hardware device be replaced in order to minimize downtime?

- Just before it's MTBF is reached
- Once every year
- Only after its first failure
- When its performance drops below 75% efficiency

Explanation

Hardware should be replaced just before its MTBF (mean time between failures) is reached. This is the statistical average time that the device will operate before experiencing its first serious failure.

Once every year is not an appropriate replacement metric, as many devices have an MTBF of 3 to 10 years or more. Waiting until a device experiences a failure does not minimize downtime; instead, that is a scheme to minimize hardware costs by using every device until failure before replacement. Waiting for a performance efficiency drop is an ineffective solution, as most hardware failures do not provide such pre-failure symptoms.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_02]

Question 3: Correct

A system failure has occurred. Which of the following restoration processes would result in the fastest restoration of all data to its most current state?

- Restore the full backup and the last incremental backup
- Restore the full backup and all differential backups
- Restore the full backup and all incremental backups
- Restore the full backup and the last differential backup

Explanation

The fastest method for restoring data to its most current state is to restore the full backup and then the last differential backup. Differential backups include all changes since the last full backup (or other backup method that resets the archive bit).

Restoring the full backup and the last incremental backup is an incomplete restore because all of the incremental backups must be used. However, restoring several backup sets rather than a single set is slower. Only the last differential backup set needs to be used.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_03]

Question 4: Correct

Which of the following are backed up during an *incremental* backup?

- Only files that have changed since the last full or differential backup.
- Only files that are new since the last full or incremental backup.
- Only files that have changed since the last full backup.
- Only files that have changed since the last full or incremental backup.

Explanation

An incremental backup will only capture files that have changed since the last full or incremental backup. The primary attraction to this backup plan is that it requires less storage space and processing time to complete the backup. Restoration starts from the last full backup and then requires the loading of each subsequent incremental backup for a full restoration.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_04]

Question 5: Correct

Which of the following are backed up during a *differential* backup?

- Only files that have been added since the last full or incremental backup.
- Only files that have changed since the last full or differential backup.
- Only files that have changed since the last full or incremental backup.
- Only files that have changed since the last full backup.

Explanation

A differential backup will only capture files that have changed since the last full backup. This backup strategy can create a shorter restoration time than an incremental backup, but may consume more disk space, depending on the frequency of full backups and the amount and frequency of file changes. Restoration is a two-step process--load the last full backup first, and then finish the restoration by loading the last differential backup.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_05]

Question 6: Correct

Which backup strategy backs up all files from a computer's file system regardless of whether the file's archive bit is set or not and marks them as having been backed up?

- Copy
- Full
- Differential
- Incremental

Explanation

A full backup backs up all files from a computer's file system regardless of whether a file's archive bit is turned on or off. It also marks them as having been backed up.

Incremental and differential backups only back up files that have their archive bit set. The copy backup strategy is used by the NTBACKUP.EXE backup utility on Windows servers. It backs up all files regardless of whether the archive bit is set. However, it does not mark them as having been backed up.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_06]

Question 7: Correct

Which backup strategy backs up only files that have the archive bit set, but does not mark them as having been backed up?

- Normal
- Full
- Incremental
- Differential

Explanation

A differential backup backs up only files that have the archive bit set, but it does not mark them as having been backed up.

A full backup backs up all files regardless of whether the archive bit is set or not. An incremental backup backs up only files that have the archive bit set, but it marks them as having been backed up. A normal backup is a type of backup unique to the NTBACKUP.EXE utility on the Windows server. It also flags the files as having been backed up.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_07]

Question 8: Correct

Your organization uses the following tape rotation strategy for its backup tapes:

1. The first set of tapes is used for daily backups.
2. At the end of each week, the latest daily backup tape is promoted to the weekly backup tape.
3. At the end of the each month, one of the weekly backup tapes is promoted to the monthly backup tape.

What kind of backup tape rotation strategy is being used?

- Differential
- Incremented tape
- Incremental
- Grandfather

Explanation

The organization is using a grandfather tape rotation scheme. This scheme involves promoting the latest son (daily) backup tape to become a father (weekly) backup tape. The latest father is promoted to become a grandfather (monthly) tape.

In the incremental tape rotation scheme, your latest backup session is stored on the oldest tape in your set. Differential is a type of backup, not a tape rotation method. In the incremented tape scheme, a set of numbered tapes is used until the end of a specified time period. Then the lowest numbered tape is removed from the set and archived. A new, high-numbered tape replaces it in the set.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_08]

Question 9: Correct

Your disaster recovery plan calls for tape backups stored at a different location. The location is a safe deposit box at the local bank. Because of this, the disaster recovery plan specifies that you choose a method that uses the fewest tapes, but also allows you to quickly back up and restore files.

Which backup strategy would best meet the disaster recovery plan for tape backups?

- Perform a full backup once per week and an incremental backup the other days of the week.
- Perform a full backup each day of the week.
- Perform a full backup once per week and a differential backup the other days of the week.
- Perform a full backup once per year and a differential backup for the rest of the days in the year.

- Perform a full backup once per month and an incremental backup the other days of the month.

Explanation

Performing a full backup once per week and a differential backup the other days of the week would best meet this disaster recovery plan. The full backup will back up all files, usually to one tape, but the backup process can be time consuming. The differential backup will back up all files since the last full backup. This backup process isn't as time consuming, and combining it with a full backup will only require two tapes to for a complete restore.

Performing a full backup each day would meet the requirement of using as few tapes as possible, but that backup process would be very time consuming each day.

Performing a full backup once per week and an incremental backup the other days of the week would be one of the fastest methods to back up files, but it would require many tapes to complete the restore. The incremental backup only backs up files added or changed since the last backup. Because of this, in order to do a complete restore of the file system, you would need a tape for each day of the week on which an incremental backup ran.

Performing a full backup once per month and an incremental backup the other days of the month would be the fastest method to backup files, but it would require many tapes to complete the restore. The incremental backup only backs up files added or changed since the last backup. Because of this, in order to do a complete restore of the file system, you would need a tape for each day of the month on which an incremental backup ran.

Performing a full backup once per year with a differential backup for the rest of the days in the year would only require two tapes for a complete file system restore, but backing up the file system would become very time consuming. The differential backup would back up everything since the last full backup.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_09]

Question 10: Correct

What does an *incremental* backup do during the backup?

- Backups up all files with the archive bit set and resets the archive bit.
- Backs up all files regardless of the archive bit and does not reset the archive bit.
- Backs up all files with the archive bit set and does not reset the archive bit.
- Backs up all files regardless of the archive bit and resets the archive bit.

Explanation

An *incremental* backup only backs up files with the archive bit set (files that have been modified). After backing up the file, the archive bit is reset. The primary attraction to this backup plan is that it requires less storage space and processing time to complete the backup. Restoration starts from the last full backup and then requires the loading of each subsequent incremental backup for a full restoration.

A *full* backup backs up all files regardless of the archive bit and resets the archive bit. A *copy* backup backs up all files without resetting the archive bit. A *differential* backup backs up all files with the archive bit set but does **not** reset the archive bit.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_10]

Question 11: Correct

What does a *differential* backup do during the backup?

- Backups up all files with the archive bit set and resets the archive bit.
- Backups up all files with the archive bit set and does not reset the archive bit.
- Backups up all files regardless of the archive bit and resets the archive bit.
- Backups up all files regardless of the archive bit and does not reset the archive bit.

Explanation

A *differential* backup backs up all files with the archive bit set (files that have been modified), but does not reset the archive bit. This backup strategy can create a shorter restoration time than an incremental backup, but may consume more disk space, depending on the frequency of full backups and the amount and frequency of file changes. Restoration is a two-step process--load the last full backup first, and then finish the restoration by loading the last differential backup.

An *incremental* backup only backs up files with the archive bit set. A *full* backup backs up all files regardless of the archive bit and resets the archive bit. A *copy* backup backs up all files without resetting the archive bit.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_11]

Question 12: Correct

Your network uses the following backup strategy:

- Full backups every Sunday night
- Incremental backups Monday night through Saturday night

On a Thursday morning, the storage system fails. How many restore operations will you need to perform to recover all of the data?

- 1
- 2
- 3
- 4
- 5

Explanation

You will need to perform four restore procedures:

1. Restore the full backup from Sunday
2. Restore the incremental backup from Monday
3. Restore the incremental backup from Tuesday
4. Restore the incremental backup from Wednesday

If you did a full backup every night, you would restore only a single backup (Wednesday's backup). If you did full backups with differential backups, you would restore the last full backup along with the last differential backup.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_12]

Question 13: Correct

Your network uses the following backup strategy:

- Full backups every Sunday night
- Differential backups Monday through Saturday nights

On Thursday morning, the storage system fails. How many restore operations will you need to perform to recover all of the data?

- 1
- 2
- 3
- 4
- 5

Explanation

You will need to perform two restore procedures:

1. Restore the full backup from Sunday
2. Restore the differential backup from Wednesday

If you did a full backup every night, you would restore only a single backup (Wednesday's backup). If you did full backups with incremental backups, you would restore the last full backup along with each incremental backup.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_13]

Question 14: Correct

Your network performs a full backup every night. Each Sunday, the previous night's backup tape is archived.

On a Wednesday morning, the storage system fails. How many restore operations will you need to perform to recover all of the data?

- 1
- 2
- 3
- 4
- 5
- 6

Explanation

You will need to perform a single restore procedure; simply restore the last full backup from Wednesday to restore all of the data.

The fact that you archive one backup each week is irrelevant to restoring the latest data. The archived copy is only used to restore something to a specific point in time. If you had used full and differential backups, you would restore the last full and last differential backups. If you had

used full and incremental backups, you would restore the last full and each subsequent incremental backup.

References

LabSim for Security Pro, Section 9.13.
[All Questions SecPro2017_v6.exm BACKUP_RESTORE_14]

Exam Report: 9.14.3 Practice Questions

Date: 6/24/2019 5:45:29 pm
Time Spent: 1:25

Candidate: Ghosh, Puja
Login: pxgst128

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following cloud storage access services acts as a gatekeeper, extending an organization's security policies into the cloud storage infrastructure?

- A web service application programming interface
- A cloud access security broker
- A co-located cloud computer service
- A cloud storage gateway

Explanation

A cloud access security broker (CASB) may act as a gatekeeper, extending an organization's security policies into the cloud storage infrastructure. A CASB focuses on the visibility of the company data, regulation compliance, user access, and data security through encryption and loss prevention.

Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API), or by applications that utilize the API, such as cloud desktop storage - a cloud storage gateway or web-based content management systems.

References

LabSim for Security Pro, Section 9.14.
[All Questions SecPro2017_v6.exm CLOUD_STOR_02]

Question 2: Correct

Which of the following is **NOT** an advantage of using cloud storage?

- Your organization can copy virtual machine images from the cloud to on-premises locations.
- Your organization can use cloud storage as a natural disaster backup.
- Your organization can purchase additional storage capacity when needed.
- Your organization can choose between off-premises and on-premises cloud storage options.
- Your organization can import a virtual machine image from an on-premises location to the cloud image library.

Explanation

Storage maintenance tasks, such as purchasing additional storage capacity, are the responsibility of the service provider.

Other advantages of cloud storage are:

- Companies only pay for the actual used storage. This does not necessarily mean that cloud storage is less expensive, but that it only incurs operating expenses.
- Cloud storage can cut energy consumption by up to 70%, making an organization more environmentally friendly.
- Organizations can choose between off-premises and on-premises cloud storage options or a mixture of the two options.
- Storage availability and data protection is intrinsic to object storage architecture, so depending on the application, the additional technology, effort and cost to add availability and protection can be eliminated.
- Cloud storage can be used for copying virtual machine images from the cloud to on-premises locations or to import a virtual machine image from an on-premises location to the cloud image library.
- Cloud storage can be used as natural disaster backup as there are normally two or three backup servers located in different places around the globe.

References

LabSim for Security Pro, Section 9.14.
[All Questions SecPro2017_v6.exm CLOUD_STOR_04]

Question 3: Correct

Which of the following is NOT a feature of the cloud storage model of data storage?

- ○ Highly durable through the creation of versioned copies.
- ○ Highly fault tolerant through redundancy and distribution of data.
- ○ Made up of many distributed resources that act as one federated or a cooperative storage cloud architecture.
- ➡ ◉ Provides access control to the file system stored in the cloud.

Explanation

Access control should be set as a local file system would be, with no need for the provider to have access to the stored data.

Cloud storage is:

- Made up of many distributed resources, but still acts as one, either in a federated or a cooperative storage cloud architecture.
- Highly fault tolerant because of redundancy and distribution of data.
- Highly durable through the creation of versioned copies.

References

LabSim for Security Pro, Section 9.14.
[All Questions SecPro2017_v6.exm CLOUD_STOR_03]

Question 4: Correct

Google Cloud, Amazon Web Services, and Microsoft Azure are some of the most widely used cloud storage solutions for enterprises. Which of the following factors prompt companies to take advantage of cloud storage? (Select two.)

- ➡ ☑ Need to bring costs down
- ☐ Need for a storage provider to manage access control
- ☐ Need for a platform as a service for developing applications

- [ ] Need for a software as a service for managing enterprise applications
- [x] Growing demand for storage

Explanation

Some of the most widely used cloud storage for enterprises are Google Cloud, Amazon Web Services, and Microsoft Azure. Because of the growing demand for storage and desire to bring costs down, many companies have been taking advantage of cloud storage.

References

LabSim for Security Pro, Section 9.14.
[All Questions SecPro2017_v6.exm CLOUD_STOR_01]

Question 5: Correct

Cloud storage is a virtual service, so the infrastructure is the responsibility of the storage provider. Access control should be set as a local file system would be, with no need for the provider to have access to the stored data.

You are implementing the following measures to secure your cloud storage:

- Verifying that security controls are the same as in a physical datacenter.
- Using data classification policies.
- Assigning information into categories that determine storage, handling, and access requirements.
- Assigning information classification based on information sensitivity and criticality.

Which of the following is another security measure you can implement?

- ( ) Configuring redundancy and distribution of data.
- ( ) Creating versioned copies of your cloud data.
- (•) Disposing of data when it is no longer needed by using specialized tools.
- ( ) Configuring distributed resources to act as one in a federated architecture.

Explanation

Disposing of data when it is no longer needed by using specialized tools is another security measure you can implement.

Creating versioned copies of your cloud data, configuring redundancy and distribution of data, and configuring distributed resources to act as one in a federated architecture are all measures that improve the fault tolerance and durability of your data.

References

LabSim for Security Pro, Section 9.14.
[All Questions SecPro2017_v6.exm CLOUD_STOR_05]