Exam Report: 8.5.10 Practice Questions

Date: 1/23/2020 6:38:55 pm
Time Spent: 4:56

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 75%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

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

➡ ○ Cookies

○ FTP

○ VPNs

● ~~HTTP~~

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 operate within a security sandbox

○ They can help a hacker spoof a user's identity

○ They can retain connection and session information

○ 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?

➡ ● Cookie

○ Mobile code

○ Digital signature

○ Certificate

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?

○ Enable the phishing filter to check all embedded links in webpages you visit

➡ ● Allow first party cookies, but block third-party cookies

○ Block cross-site scripting (XSS)

○ Prevent ActiveX controls and Java on linked websites

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*?

○ An executable file that runs in the background and tracks internet use.

○ A malicious program that disguises itself as a useful program.

➡ ● A file saved on your hard drive that tracks website preferences and use.

○ A malicious program that runs when you read an email attachment.

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

○ Not use any public computer that has been used in the last 30 minutes

➡ ● Clear the browser cache

○ Ensure that public login credentials are unique

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?

○ Change the filter level in Pop-up Blocker to High.

➡ ● Add the URL of the website to the Local intranet zone.

○ Change the filter level in Pop-up Blocker to Medium.

○ In Internet Options, use the Privacy tab to turn off Pop-up Blocker.

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: Incorrect

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]