Exam Report: 13.3.12 Practice Questions

Date: 5/26/2020 6:57:43 pm
Time Spent: 5:29

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 25%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Which of the following mobile security concerns is characterized by malicious code that specifically targets mobile devices?

➡ ● Malicious websites

○ Unsecure applications

○ Phishing attacks

○ Lost and stolen devices

Explanation

Malicious or compromised websites are often used to launch web or network attacks. An attacker can design a website to easily determine what type of device is being used and then use malicious code that specifically targets mobile devices.

Phishing and other social engineering attacks are often more productive on mobile device users, but are not characterized by malicious code that specifically targets mobile devices.

Data loss can occur when a mobile device is lost or stolen, but is not characterized by malicious code that specifically targets mobile devices.

Unsecure applications are a security concern since mobile apps may not have the same security protections as a browser, but they are not characterized by malicious code that specifically targets mobile devices.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICE_ATTACKS_SECURITY_CONCERNS_01_EH1]

Question 2: Incorrect

Which key area in the mobile device security model is supported by device designers requiring passwords, biometrics, and two-factor authentication methods?

○ Isolation

○ Digital signing

● ~~Encryption~~

➡ ○ Access controls

Explanation

Access control includes passwords, biometrics, and two-factor authentication methods to gain access to the device.

Only digitally signed apps should be installed. A digital signature verifies that an app hasn't been tampered with and verifies that the app came from the original author.

Encryption can be used to secure communications to and from a mobile device and to securely store information on a mobile device.

Isolation refers to a mobile device's application sandbox that forces applications to run as a separate process.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICE_ATTACKS_SECURITY_FEATURES_01_EH1]

Question 3: Incorrect

Which of the following describes the risks of spyware that are particular to mobile devices?

● ~~Spyware can crack weak passwords.~~

○ Spyware can exploit applications that have not been patched.

➡ ○ Spyware can monitor and log call histories, GPS locations, and text messages.

○ Spyware can root or jailbreak a mobile device.

Explanation

Spyware apps can monitor and log activity on a mobile device, including:

- Call history
- GPS location
- Text messages
- Email
- Keystrokes

Weak passwords can make a model device vulnerable, but spyware doesn't crack weak passwords.

Unpatched applications can make a model device vulnerable, but spyware doesn't exploit unpatched applications.

Spyware doesn't root or jailbreak mobile devices.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICE_ATTACKS_THREATS_01_EH1]

Question 4: Correct

Which of the following operating systems is the most prevalent in the smartphone market?

○ Windows

○ Blackberry

➡ ● Android

○ iOS

Explanation

Essentially, only two operating systems share the smartphone market, Android and iOS, with Android having the largest share.

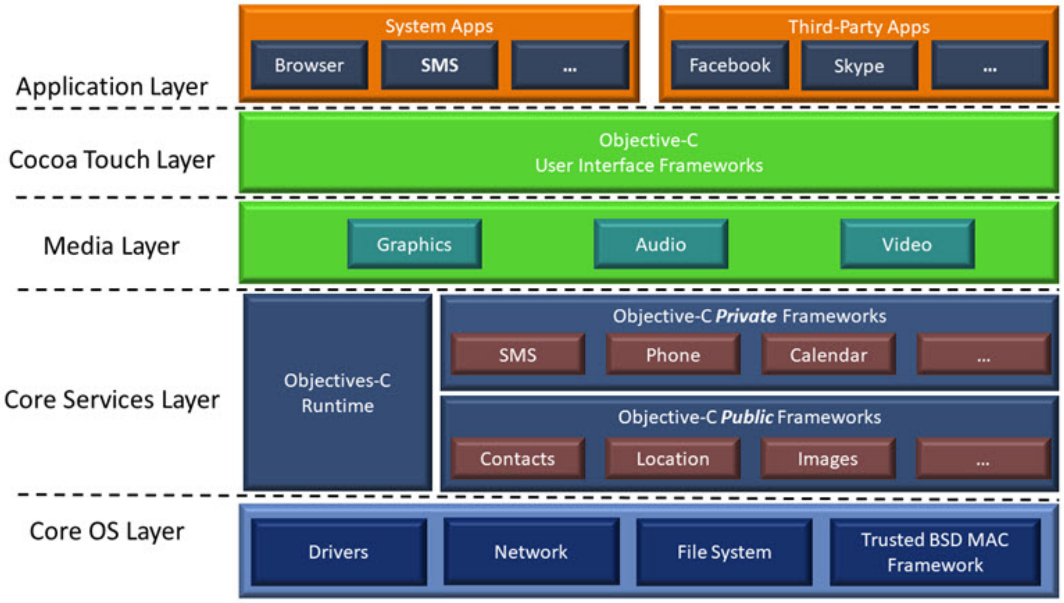
Windows, Blackberry, and Palm OS each have less than one percent of the smartphone market share.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_OS_01_EH1]

Question 5: Incorrect

Which of the following best describes this image?



➡ ○ The iOS operating system stack.

○ The operating system layers that can be overcome by rooting or jailbreaking.

● ~~The Android Application Programming Interfaces (APIs).~~

○ The Mobile Security Model.

Explanation

The image represents the iOS operating system stack.

The Android Application Programming Interfaces (APIs) are associated with the Android Framework layer of the Android stack.

The Mobile Security Model includes the following areas:

- Access control
- Digital signing
- Encryption
- Isolation
- Permissions-based access controls

Rooting or jailbreaking overcomes the security restrictions imposed by the device's manufacture. Generally, this is done to make changes to the upper layers only.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_OS_IOS_STACK_01_EH1]

Question 6: Incorrect

Linda, an Android user, wants to remove unwanted applications (bloatware) that are pre-installed on her device. Which of the following actions must she take?

○ Jailbreak the Android device.

○ Sideload the unwanted applications.

● ~~Run a Settings application with administrative privileges.~~

➡ ○ Root the Android device.

Explanation

Rooting overcomes the security restrictions imposed by the Android device's manufacturer to:

- Visually change the appearance or theme.
- Increase performance by overclocking the CPU or GPU.
- Remove bloatware that comes pre-installed on the device.

Sideloading is the installation of an app on a mobile device outside of the official application distribution methods. Android allows sideloading, but may give you a warning.

Overcoming security restrictions imposed by the Android device's manufacturer is called rooting. Jailbreaking overcomes the security restrictions imposed by an iOS device.

Running a settings application with administrative privileges will not allow a user to remove unwanted applications.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_OS_ROOT_JAILBREAK_01_EH1]

Question 7: Incorrect

Which of the following can void a mobile device's warranty, cause poor performance, or brick a mobile device (making it impossible to turn on or repair)?

● ~~Third party applications~~

➡ ○ Rooting or jailbreaking

○ Digital signing

○ Permissions-based access controls

Explanation

Rooting or jailbreaking a mobile device may:

- Void the device's warranty
- Cause poor performance
- Incur malware infections
- Brick the device making it impossible to turn on or repair.

Both Android and iOS devices allow third-party applications from approved sources.

Digital signing and permissions-based access controls are areas of the mobile security model.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_OS_ROOT_JAILBREAK_02_EH1]

Question 8: Incorrect

Jose, a medical doctor, has a mobile device that contains sensitive patient information. He is concerned about unauthorized access to the data if the device is lost or stolen. Which of the following is the best option for preventing this from happening?

➡ ○ Configure the device to remotely wipe as soon as it is reported lost.

○ Install a locator application on the device so that it can be traced.

○ Configure the device for multifactor authentication.

● ~~Configure the device to wipe after a number of failed login attempts.~~

Explanation

Mobile devices can be configured to be perform a factory reset or wipe when the device is reported lost or stolen. This is the best of the presented options.

Configuring the device for multifactor authentication will make it harder to hack, but is not the best solution presented.

Installing a locator application on the device makes it possible to trace, but is not the best solution presented.

Configuring the device to wipe after a number of failed login attempts is a good solution, but not the best solution presented.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_HACKING_BEST_PRACTICE_01_EH1]

▼ **Question 9:** Incorrect

Which of the following mobile security best practices for users is concerned with geotags?

➡ ○ Don't auto-upload photos to social networks.

● ~~Configure a passcode to access the mobile device.~~

○ Don't install too many applications.

○ Don't root or jailbreak the mobile device.

Explanation

Don't auto-upload photos to social networks. Uploading photos is a privacy concern, and photos have geotags that can be used to track movements.

Photos may have geotags; passcodes don't.

Rooting and jailbreaking don't involve geotags.

Installing too many applications may take up storage and incur additional vulnerabilities, but installing apps doesn't involve geotags.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_HACKING_BEST_PRACTICE_02_EH1]

▼ **Question 10:** Incorrect

Which of the following policies best governs the use of bring-your-own-device (BYOD) that connect with an organization's private network?

➡ ○ Acceptable use policy

○ Cloud usage policy

○ Remote management policy

● ~~Remote wipe policy~~

Explanation

An acceptable use policy governs all aspects of the use of BYOD that connect with an organizations private network.

A cloud usage policy governs the applications that connect to cloud resources and cloud data storage whether or not a BYOD device is connected to an organization's private network.

Enabling remote management is a mobile security best practice for users. It may be part of the acceptable use policy, but is not the best answer.

Setting up remote wipe is a mobile security best practice for users. It may be part of the acceptable use policy, but is not the best answer.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_HACKING_BEST_PRACTICE_03_EH1]

▼ **Question 11:** Incorrect

James, a penetration tester, uses nmap to locate mobile devices attached to a network. Which of the following mobile device penetration testing stages is being implemented?

- ◉ ~~Scanning~~
- ○ Exploitation
- ○ Post-exploitation
- ➡ ○ Footprinting

Explanation

Footprinting uses scanning tools like nmap to locate mobile devices attached to your network. These tools often return the OS version and type.

Scanning uses software like Kismet to find which wireless networks the devices are looking for.

Exploitation uses man-in-the-middle attacks, spoofing, ARP poisoning, and traffic insertion attacks to exploit client-side vulnerabilities and manipulate captured traffic to exploit back-end servers.

During post-exploitation, data areas on the mobile device are inspected for sensitive information.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_HACKING_PEN_TEST_01_EH1]

▼ Question 12: Incorrect

Which of the following describes the exploitation stage of the mobile device penetration testing process?

- ○ The inspection of data areas on the mobile device for sensitive information.
- ○ The use of scanning tools to determine which wireless networks the mobile device is looking for.
- ◉ ~~The use of scanning tools to locate mobile devices attached to your network.~~
- ➡ ○ The use of man-in-the-middle attacks, spoofing, and other attacks to take advantage of client-side vulnerabilities.

Explanation

Exploitation uses man-in-the-middle attacks, spoofing, ARP poisoning, and traffic insertion attacks to exploit client-side vulnerabilities and manipulate captured traffic to exploit back-end servers.

Footprinting uses scanning tools like nmap to locate mobile devices attached to your network. These tools often return the OS version and type.

Scanning uses software like Kismet to find which wireless networks the devices are looking for.

During post-exploitation, data areas on the mobile device are inspected for sensitive information.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_HACKING_PEN_TEST_02_EH1]

▼ Question 13: Incorrect

Which of the following steps in an Android penetration test checks for a vulnerability hackers use to break down the browser's sandbox using infected JavaScript code?

- ◉ ~~Detect capability leaks~~
- ➡ ○ Check for a cross-application-scripting error
- ○ Exploit the Android Intents system
- ○ Check for unencrypted email passwords

Explanation

Checking for a cross-application-scripting error requires investigating vulnerabilities in the Android browser. Hackers use this vulnerability to break down the browser's sandbox using infected JavaScript code.

Checking for unencrypted email passwords and Skype contacts involves data stored in the SQLite database, not infected JavaScript code.

Exploiting the Android Intents system involves using the APSET tool to gain the user's private information. Android Intents is a messaging system that is used by Android apps to request functionality from other Android components.

Detecting capability leaks does not involve infected JavaScript code.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MOBILE_DEVICES_HACKING_PEN_TEST_03_EH1]

▼ Question 14: Incorrect

Which of the following bring-your-own-device (BYOD) risks is both a security issue for an organization and a privacy issue for a BYOD user?

○ Work flexibility

○ Lower cost

➡ ○ Mixing personal and corporate data

● ~~Confidential data exposure~~

Explanation

Mixing personal and corporate data is both a security issue for a company and a privacy issue for users.

Confidential data exposure can occur when a mobile device synchronizes with organization email and other cloud-connected apps to download corporate and confidential information. This is a risk to the organization, but not the user.

Lower cost is a benefit of BYOD, not a security issue.

Work flexibility is a benefit of BYOD, not a security issue.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MDM_BYOD_01_EH1]

▼ Question 15: Correct

Which of the following describes Mobile Device Management software?

○ An application that allows a mobile device to be used for both professional and personal needs.

○ The policy that specifies the acceptable use of mobile devices supplied by an organization and bring-your-own-devices (BYOD).

➡ ● A combination of an on-device application or agent that communicates with a backend server to receive policies and settings.

○ The policies and procedures used by an organization to maintain security and permissions on mobile devices.

Explanation

MDM software is typically deployed as a combination of an on-device application or agent that communicates with a backend server.

The term Mobile Device Management (MDM) is generally used to describe the policies and procedures used by an organization to maintain security and permissions on mobile devices. This does not describe MDM software.

Bring-your-own-device (BYOD) is described as a mobile device used for both professional and personal needs.
The policy that specifies the acceptable use of mobile devices supplied by an organization and bring-your-own-devices (BYOD) is the Acceptable Use policy.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MDM_MDM_01_EH1]

Question 16: Correct

Alan, an ethical hacker, roots or jailbreaks a mobile device. He checks the inventory information reported by the mobile device management (MDM) software that manages the mobile device. Which of the following describes what he expects to see in the inventory?

➡ ● The inventory will show the device as vulnerable.

○ The inventory will show that all data has been removed from the device.

○ The inventory will show that a device lockout has occurred, preventing anyone from using the device.

○ The inventory will show that a password is no longer needed to access the device.

Explanation

An MDM should flag a mobile device as vulnerable when it is rooted or jailbroken.

All data is removed from a device when the MDM software performs a remote wipe.

An MDM can enforce a policy the requires a passcode. This will not be shown in an inventory.

An MDM can enforce a policy to lock a device, preventing anyone from using the device. This will not be shown in an inventory.

References

TestOut Ethical Hacker Pro - 13.3 Mobile Devices
[e_mobile_devices_eh1.exam.xml Q_MDM_MDM_02_EH1]