Exam Report: 14.2.12 Practice Questions

Date: 5/26/2020 7:14:29 pm
Time Spent: 0:33

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following has five layers of structure that include Edge technology, Access gateway, Internet, Middleware, and Application?

- IoT structure
- ~~IoT systems~~
- IoT architecture
- IoT application areas and devices

Explanation

The IoT has been structured into an architecture of layers because with so many devices operating in one system and this system being connected with other processes, IoT needs a well-defined and effective architecture to function properly. The layers help track the consistency of the system. There are five layers total: Edge technology, Access gateway, Internet, Middleware, and Application.

IoT systems involves grouping technology in four categories: devices, gateway system, data storage system using cloud, and remote control through mobile apps.

IoT application areas and devices explores the sectors in society using IoT, which devices each sector uses, and how the devices are used.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_IOT_ARCHIT_01_EH1]

Question 2: Incorrect

What are the four primary systems of IoT technology?

- Devices, sensors, apps, and internet
- Devices, gateway, data storage, and remote control
- Devices, data storage, remote control, and internet
- ~~Devices, gateway, sensors, and apps~~

Explanation

IoT technology comprises four primary systems: devices, gateway system, data storage system using cloud, and remote control through mobile apps.

Sensors are hardware included in many IoT devices.

Apps are part of the remote control system.

Internet is part of the gateway and data storage systems.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_IOT_SYSTEM_01_EH1]

Question 3: Correct

Anabel purchased a smart speaker. She connected it to all the smart devices in her home. Which of the following communication models is she using?

- Device-to-gateway
- Device-to-device
- Back-end data-sharing
- Device-to-cloud

Explanation

The device-to-device model is meant mostly for systems with devices transferring small data packets to each other at a very low data rate. The devices could include thermostat, light bulbs, door locks, CCTV cameras, refrigerators, and wearable devices.

The device-to-gateway model means that the IoT device doesn't directly interact with the cloud or the client. Instead, the device interacts with an intermediate device, or gateway, which then contacts the cloud to send and receive data.

The back-end data-sharing model is an expanded version of the device-to-cloud model. This means the data sent from the IoT device to the cloud can be accessed by authorized third parties.

The device-to-cloud model means that the devices communicate with the cloud instead of directly with the end user to send data and receive commands.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_TECH_PROTO_COMM_MODELS_01_EH1]

Question 4: Correct

YuJin drove his smart car to the beach to fly his drone in search of ocean animal activity. Which of the following operation systems are most likely being used by his car and drone?

- Integrity RTOS and snappy
- ARM mbed OS and snappy
- Contiki and integrity RTOS
- RIOT OS and brillo

Explanation

Nucleus and Integrity RTOS are both used in the aerospace, industrial, automotive, and medical sectors.

Snappy, or Ubuntu Core, is used for drones, robots, and so on.

RIOT OS requires less resources and is energy efficient. It's used on embedded systems, actuator boards, sensors, and so on.

ARM mbed OS is used primarily with low-power devices such as wearable devices.

Brillo is an Android-based embedded OS. It's used for low-end devices.

Contiki is used for low-power wireless devices, including street lighting and monitoring systems.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_TECH_PROTO_OP_SYS_01_EH1]

Question 5: Correct

Which of the following is a short-range wireless personal area network that supports low-power, long-use IoT needs?

- Wi-Fi
- Li-Fi
- BLE
- IoE

Explanation

Bluetooth low energy (BLE), also known as Bluetooth Smart, is a wireless personal area network. It supports low-power, long-use IoT needs.

IoE, or the internet of everything, is another name for IoT.

Light-Fidelity, or Li-Fi, is very similar to Wi-Fi. The two key differences are speed and mode of communication. Unlike Wi-Fi, Li-Fi is a Visible Light Communications system. It uses light bulbs to transfer data at a high speed of 224 Gigabits per second.

Wi-Fi is commonly implemented in wireless local area networking. The most common Wi-Fi standard is the 802.11n standard, with a maximum speed of 600 Megabits per second and a range of about 50 meters.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_TECH_PROTO_SHORT-RANGE_01_EH1]

Question 6: Incorrect

Which of the following attacks utilizes encryption to deny a user access to a device?

- HVAC attack
- DoS
- ~~DDoS attack~~
- Ransomware attack

Explanation

In a ransomware attack, the hacker utilizes encryption to deny a user access to its device by locking files or even the screen.

In a DDoS attack, the hacker exploits vulnerabilities to take over and use all the devices in the IoT network as a zombie army to target a server or system, making the services unavailable.

Hackers exploit HVAC systems to retrieve confidential information from users as well as to take over a network.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_CHALLENGES_ATTACK_01_EH1]

Question 7: Incorrect

Which of the following is a nonprofit organization that provides tools and resources for web app security and is made up of software developers, engineers, and freelancers?

- OWASP
- HaLow
- ~~beSTORM~~
- KillerBee

Explanation

OWASP stands for Open Web Application Security Project. It is a nonprofit organization made up of software developers, engineers, and freelancers. They provide tools and resources for web app security. From time to time, OWASP publishes a report on the 10 most serious web app security risks affecting the cyber world.

KillerBee is a tool that specializes in attacking Zigbee and IEEE 802.15.4 networks.

beSTORM is a smart fuzzer that finds buffer overflow weaknesses as it automates and documents the process of delivering malicious input and then watches for unpredicted responses from an application.

HaLow is a branch of Wi-Fi with extended range. It's most useful in rural areas because it uses low data rates, reducing transmission power requirements and cost.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_CHALLENGES_OWASP_VULN_01_EH1]

Question 8: Incorrect

Joelle, an app developer, created an app using two-factor authentication (2FA) and requires strong user passwords. Which of the following IoT security challenges is she trying to overcome?

- ~~Difficulty updating firmware and OS~~
- Default, weak, and hardcoded credentials
- Cleartext protocols and open ports
- Lack of security and privacy

Explanation

Many IoT devices allow weak or default passwords, which are easy to attack and break. The main problem is that there's no set regulation for IoT authentication, only guidelines. Some ways to strengthen IoT devices with authentication are to use two-factor authentication (2FA) and enforce strong passwords or certificates.

Most IoT devices and services lack the most basic security and privacy policies required to protect all this data being gathered. It's imperative to store and process data securely across the network. This means redacting or anonymizing sensitive data before storing it.

There are a few reasons why updates to IoT devices happen rarely, if at all. Each device should undergo proper testing before being released to the market, and updates should happen regularly.

Most data in the IoT network is transferred and received as cleartext. This makes the data extremely weak against theft, breaches, and other malicious acts.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_CHALLENGES_SECURITY_01_EH1]

Question 9: Correct

Which of the following is the correct order for a hacker to launch an attack?

- Vulnerability scanning, information gathering, gain remote access, launch attack, maintain access
- Information gathering, vulnerability scanning, launch attack, gain remote access, maintain access
- Launch attack, information gathering, vulnerability scanning, gain remote access, maintain access
- Gain remote access, maintain access, vulnerability scanning, information gathering, launch attack

Explanation

Hackers first gather information on the target they intend to exploit. Then they scan the network or system for vulnerabilities worth attacking. Next, they launch the attack. During the attack, their goal is to gain access to a device, then command and control the attack while remaining undetected by security products. Finally, the hacker tries to maintain access for as long as possible to launch more elaborate attacks.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_HACKING_METHOD_01_EH1]

Question 10: Incorrect

During a penetration test, Omar found unpredicted responses from an application. Which of the following tools was he most likely using while assessing the network?

- Censys
- Zniffer
- beSTORM
- ~~Shodan~~

Explanation

beSTORM is a smart fuzzer that finds buffer overflow weaknesses as it automates and documents the process of delivering malicious input and then watches for unpredicted responses from an application.

Censys is a public search engine and data processing company that gets their data by scanning the Internet continuously.

Zniffer is a hardware tool that finds smart device traffic in a network.

Shodan is a tool that can search the Internet and gather information about potential targets.

References

TestOut Ethical Hacker Pro - 14.2 Internet of Things
[e_iot_eh1.exam.xml Q_IOT_HACKING_TOOLS_01_EH1]