

Question 1

Correct

Mark 2.00 out of 2.00

Flag question

True or False?

On some home routers, to compromise the security on the router, a Flash applet can be used to change the DNS server settings with an UPnP request.

Select one:

- ☒ true
- ☐ false



Refer to curriculum topic: 5.1.3

On some home routers, security can be compromised by running a Flash applet which can change the DNS server settings when an UPnP request is made. This could be used to redirect legitimate traffic to malevolent websites.

The correct answer is: true

[Show one page at a time](#)[Finish review](#)

Question 2

Correct

Mark 2.00 out of 2.00

Flag question

Which attack involves a compromise of data that occurs between two end points?

Select one:

- ☐ username enumeration
- ☐ denial-of-service
- ☐ extraction of security parameters
- ☒ man-in-the-middle attack



Refer to curriculum topic: 5.1.1

Threat actors frequently attempt to access devices over the internet through communication protocols. Some of the most popular remote exploits are as follows:

- **Man-In-the-middle attack (MITM)** – The threat actor gets between devices in the system and intercepts all of the data being transmitted. This information could simply be collected or modified for a specific purpose and delivered to its original destination.
- **Eavesdropping attack** – When devices are being installed, the threat actor can intercept data such as security keys that are used by constrained devices to establish communications once they are up and running.
- **SQL injection (SQLi)** – Threat actors use a flaw in the Structured Query Language (SQL) application that allows them to have access to

Question **3**


Correct

Mark 2.00 out of
2.00

🚩 Flag
question

What is a characteristic of the constrained application protocol (CoAP)?

Select one:

- ☒ It allows for efficient sensor and node communication without requiring a centralized control mechanism. 
- ☐ It is mostly used for multiple clients where live data is the only data.
- ☐ It supports the last will and testament option.
- ☐ It is primarily designed to collect data from many devices and deliver that data to the IT infrastructure.

Refer to curriculum topic: 5.1.3

CoAP uses a client-server model that allows for efficient sensor and node communication. CoAP is a lightweight protocol that uses UDP (but can use TCP) and is mainly used for M2M communication.

The correct answer is: It allows for efficient sensor and node communication without requiring a centralized control mechanism.

Question **4**


Correct

Mark 2.00 out of
2.00

🚩 Flag
question

What is a characteristic of the message queueing telemetry transport (MQTT) protocol?

Select one:

- ☒ The MQTT protocol requires a message broker. 
- ☐ It is designed to connect servers together.
- ☐ MQTT uses the User Datagram Protocol.
- ☐ It is mainly used for instant messaging.

Refer to curriculum topic: 5.1.3

MQTT requires a message broker that manages communication between publisher and subscriber clients.

The correct answer is: The MQTT protocol requires a message broker.

Question 5

Correct

Mark 2.00 out of 2.00

🚩 Flag question

What is a characteristic of the Constrained Application Protocol (CoAP)?

Select one:

- ☐ It is an inefficient messaging protocol.
- ☐ It is designed to connect servers together.
- ☒ It is a document transfer protocol.
- ☐ It uses the TCP protocol.



Refer to curriculum topic: 5.1.3

CoAP (Constrained Application Protocol) is a document transfer protocol that utilizes the User Datagram Protocol (UDP).

The correct answer is: It is a document transfer protocol.

Question 6

Correct

Mark 2.00 out of 2.00

🚩 Flag question

What is a characteristic of Extensible Messaging and Presence Protocol (XMPP)?

Select one:

- ☐ It uses a publish-subscribe Model and supports the last will and testament option.
- ☐ It uses UDP for efficient packet sizes.
- ☒ It uses an addressing scheme (name@domain.com) which helps simplify connections.
- ☐ It uses a client-server model to inform clients of state changes as they occur.



Refer to curriculum topic: 5.1.3

XMPP uses an addressing scheme (name@domain.com) to simplify connections and enable communication when data is sent between distant points.

The correct answer is: It uses an addressing scheme (name@domain.com) which helps simplify connections.

Question 7

Correct

Mark 2.00 out of 2.00

Flag question

Which password is the most hardened password for use on an IoT device?

Select one:

- ☐ 12gnkjl9!!!ddfg
- ☒ Hnmmmkoty#4
- ☐ ajkyfrjn0999y*
- ☐ 1245rdghy67#



Refer to curriculum topic: 5.2.1

Hardened passwords should consist of at least 12 characters with a combination of uppercase, lowercase, numbers, and special characters.

The correct answer is: Hnmmmkoty#4

Question 8

Correct

Mark 2.00 out of 2.00

Flag question

A threat actor has placed a rogue device on the network to manipulate the chosen destination of all packets. Which remote exploit was used by the threat actor?

Select one:

- ☐ denial-of-service
- ☒ routing attack
- ☐ username enumeration
- ☐ extraction of security parameters



Refer to curriculum topic: 5.1.1

Threat actors frequently attempt to access devices over the internet through communication protocols. Some of the most popular remote exploits are as follows:

- **Man-In-the-middle attack (MITM)** – The threat actor gets between devices in the system and intercepts all of the data being transmitted.

Question 9

Correct

Mark 2.00 out of 2.00

Flag question

What is the safest way to prevent an XXE attack?

Select one:

- ☐ Use SSL encryption on all traffic between the server and external clients.
- ☐ Use hardened passwords with a minimum of 12 characters.
- ☐ Use Pass phrases instead of a password.
- ☒ Disable XML external entity and DTD processing in the application.



Refer to curriculum topic: 5.2.1

An XXE attack can be prevented by disabling XML external entity and DTD processing in the application.

The correct answer is: Disable XML external entity and DTD processing in the application.

Question 10

Correct

Mark 2.00 out of 2.00

Flag question

A threat actor has injected JavaScript code into the output of a web application and is manipulating client-side scripts to run as desired in the browser. Which web front-end vulnerability is the threat actor exploiting?

Select one:

- ☐ security misconfiguration
- ☐ broken authentication
- ☒ cross-site scripting
- ☐ SQL injections



Refer to curriculum topic: 5.1.2

Web front-end vulnerabilities apply to apps, APIs, and services. Some of the most significant vulnerabilities are as follows:

- **Cross-site scripting:** In a cross-site scripting (XSS) attack, the threat actor injects code, most often JavaScript, into the output of a web application. This forces client-side scripts to run the way that the threat actor wants them to run in the browser.
- **SQL injections:** In an SQLi the threat actor targets the SQL database itself, rather than the web browser. This allows the threat actor to control the application database.

Question 11

Correct

Mark 2.00 out of 2.00

Flag question

For which type of devices is the use of DDS (data distribution service) in M2M connections well suited?

Select one:

- ☐ for devices that require subscription of data on a server referred to as a broker
- ☒ for devices that measure real-time data in microseconds that need to be filtered and delivered efficiently
- ☐ for devices where live data is not the only data and which use a client-server model
- ☐ for devices that require a collection of data for centralized storage and filtration



Refer to curriculum topic: 5.1.3

Devices that measure real-time data in microseconds are good candidates for DDS (data distribution service). DDS will filter the data and send the required data efficiently to endpoints requiring it. DDS is the protocol of choice when dealing with applications that require speed and reliability.

The correct answer is: for devices that measure real-time data in microseconds that need to be filtered and delivered efficiently

Question 12

Correct

Mark 2.00 out of 2.00

Flag question

What is a characteristic of the message queueing telemetry transport (MQTT) publish-subscribe model?

Select one:

- ☐ The last will and testament option allows for immediate session termination, thus saving power.
- ☐ Clients are prevented from subscribing to any subtopics in order to keep traffic to a minimum.
- ☒ It allows for a retained messages option that can be used to provide status updates.
- ☐ Clients that are connected will prevent other clients from connecting, thus preserving power.



Refer to curriculum topic: 5.1.3

MQTT is used for machine to machine (M2M) IoT communications and has an option to retain messages that can be used to provide status updates. MQTT allows clients to receive many messages when subscribed to a topic within subtopics. It also supports an option called the last will and testament option that ensures that the client receives the most current updates of the topics subscribed to. Clients connected do not prevent other clients from connecting and the traffic model that is used helps to keep traffic to a minimum, thus enabling reduction in power.

The correct answer is: It allows for a retained messages option that can be used to provide status updates

Question 13

Correct

Mark 2.00 out of 2.00

Flag question

Which popular exploit used by threat actors intercepts a system update and injects an update of their own?

Select one:

- ☐ SQL injections
- ☐ eavesdropping attack
- ☐ routing attack
- ☒ firmware replacement



Refer to curriculum topic: 5.1.1

Some of the most popular local exploits targeted by threat actors are as follows:

- **Firmware Replacement** – Updates and patches to devices are usually done remotely. If the process is not secure, threat actors could intercept the update and install their own malicious update. They could have full control over the device and begin attacking other devices in the system.
- **Cloning** – By creating a duplicate device, both in physical form and the software and firmware running on that device, the threat actor could replace a legitimate device. When the device is up and running, the threat actor could then steal information, or compromise additional devices.
- **Denial of service (DoS)** – The threat actor could launch a DoS attack to fill the communications channel, causing devices to respond to requests late, or not at all. Depending on the devices, this could cause a lot of damage.
- **Extraction of Security Parameters** – When a device is not protected properly, the threat actor may be able to extract security parameters from it such as authentication information or security keys.

The correct answer is: firmware replacement

Question 14

Correct

Mark 2.00 out of 2.00

Flag question

Which popular exploit used by threat actors fills the communications channel so that the targeted device responds to requests late or not at all?

Select one:

- ☐ phishing
- ☒ DoS
- ☐ routing attack



Question **15**

Correct

Mark 2.00 out of
2.00

🚩 Flag
question

What is a commonly exposed mobile application vulnerability?

Select one:

- ☐ malware
- ☐ user enumeration
- ☐ SQL injections
- ☒ insecure data storage



Refer to curriculum topic: 5.1.1

Threat actors can gain access and control mobile devices through compromised mobile applications, even though both Android and iOS are relatively secure. Some of the most widely exposed vulnerabilities are as follows:

- **Insecure communication** – The communication technology and channel must be secured. When there is weak negotiation, poor handshake practices, and the use of incorrect versions of SSL, the communication is not secure.
- **Insecure data storage** – Many applications have access to data storage areas of mobile devices, even though they may not need it. Data storage must be secured and applications must be tested to ensure there is no data leakage.
- **Insecure authentication** – A session must be managed properly to ensure that it is performed securely. Users must be identified when necessary, and their identity must be maintained securely.
- **Improper platform usage** – Mobile apps use features built into the platforms such as TouchID, Keychain, and Android intents. Should these security controls be misused, access to the device and other apps can be compromised.
- **Insufficient cryptography** – The cryptography used to encrypt sensitive data must be sufficient and must be applied when necessary.

The correct answer is: insecure data storage

[Finish review](#)

◀ [Chapter 5 Terms and Concepts Practice](#)

Jump to...



[Read Chapter 6: Vulnerability and Risk
Assessment in an IoT System](#) ▶