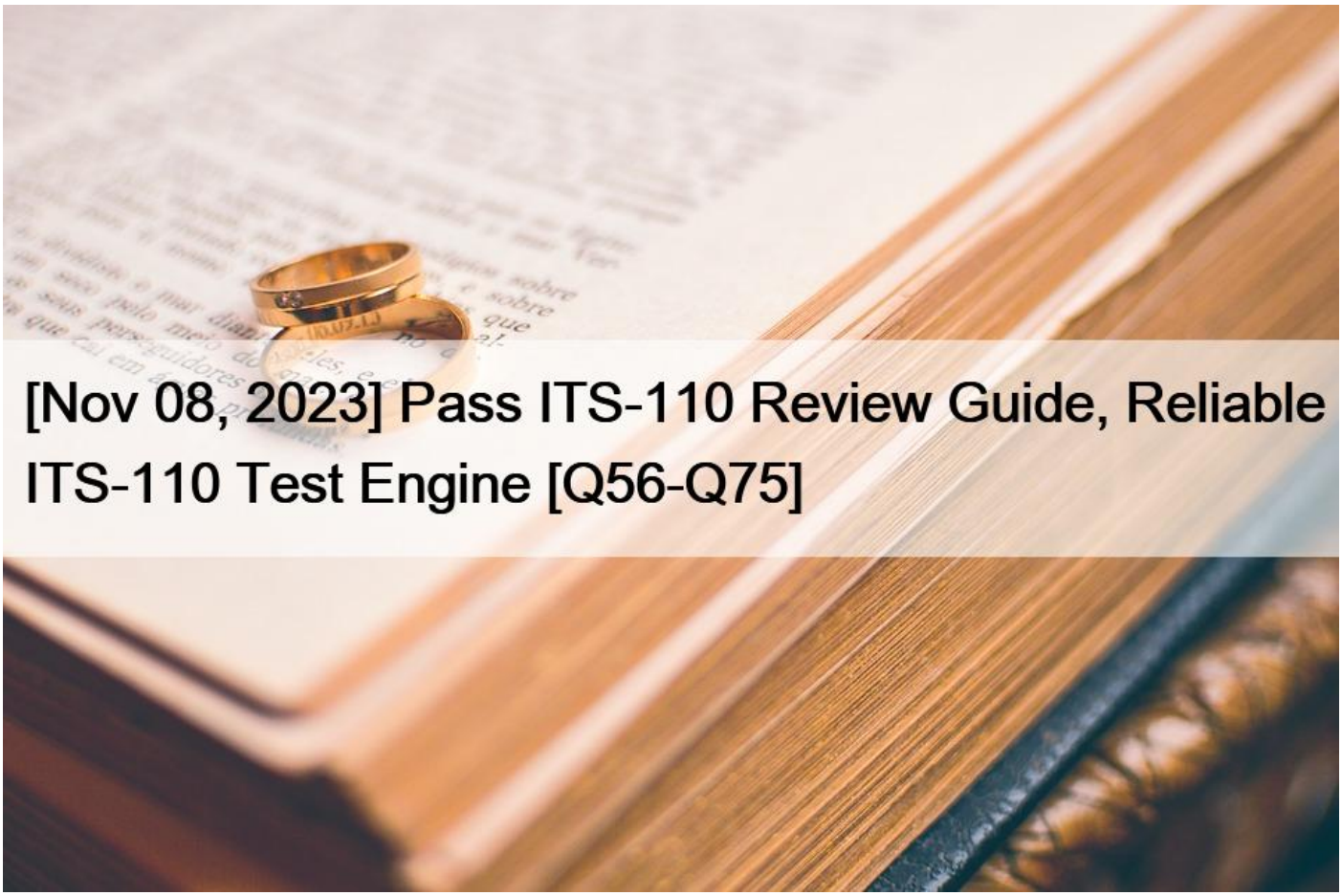
[Nov 08, 2023 Pass ITS-110 Review Guide, Reliable ITS-110 Test Engine [Q56-Q75



[Nov 08, 2023] Pass ITS-110 Review Guide, Reliable ITS-110 Test Engine
ITS-110 Test Engine Practice Test Questions, Exam Dumps

The IoT has taken over many industries, and the demand for IoT-enabled devices continues to grow every day. However, the IoT ecosystem is highly vulnerable to cyberattacks because of the interconnection of devices to the internet. This vulnerability puts the data and privacy of individuals and businesses at risk, which underscores the importance of having an IoT security expert. The ITS-110 certification provides individuals with the necessary knowledge and skills to protect the IoT ecosystem from cyber threats, making them highly sought-after professionals in the IT industry.

The ITS-110 certification exam covers a range of topics that include IoT architecture, IoT security, and privacy, and threat management among others. Candidates who wish to earn the certification must pass a rigorous exam that tests their competencies in various areas. ITS-110 exam consists of 75 multiple-choice questions that must be answered within 90 minutes, and the passing score is 70%.

Q56. A security practitioner wants to encrypt a large datastore. Which of the following is the BEST choice to implement?
* Asymmetric encryption standards
* Symmetric encryption standards
* Elliptic curve cryptography (ECC)
* Diffie-Hellman (DH) algorithm

Q57. An IoT security architect needs to secure data in motion. Which of the following is a common vulnerability used to exploit unsecure data in motion?
* External flash access
* Misconfigured Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
* Databases and datastores
* Lack of memory space isolation

Q58. A developer needs to implement a highly secure authentication method for an IoT web portal. Which of the following authentication methods offers the highest level of identity assurance for end users?
* A hardware-based token generation device
* An X.509 certificate stored on a smart card
* Two-step authentication with complex passwords
* Multi-factor authentication with three factors

Q59. An embedded developer is about to release an IoT gateway. Which of the following precautions must be taken to minimize attacks due to physical access?
* Allow access only to the software
* Remove all unneeded physical ports
* Install a firewall on network ports
* Allow easy access to components

Q60. Which of the following attacks relies on the trust that a website has for a user’s browser?
* Phishing
* SQL Injection (SQLi)
* Cross-Site Scripting (XSS)
* Cross-Site Request Forgery (CSRF)

Q61. Which of the following methods or technologies is most likely to be used to protect an IoT portal against protocol fuzzing?
* Secure Hypertext Transfer Protocol (HTTPS)
* Public Key Infrastructure (PKI)
* Next-Generation Firewall (NGFW)
* Hash-based Message Authentication Code (HMAC)

Q62. A manufacturer wants to ensure that approved software is delivered securely and can be verified prior to installation on its IoT devices. Which of the following technologies allows the manufacturer to meet this requirement?
* Advanced Encryption Standard (AES)
* Public Key Infrastructure (PKI)
* Generic Routing Encapsulation (GRE)
* Internet Protocol Security (IPsec)

Q63. A hacker is able to access privileged information via an IoT portal by modifying a SQL parameter in a URL. Which of the following BEST describes the vulnerability that allows this type of attack?
* Unvalidated redirect or forwarding
* Insecure HTTP session management

* Unsecure direct object references
* Unhandled malformed URLs

Q64. A software developer for an IoT device company is creating software to enhance the capabilities of his company’s security cameras. He wants the end users to be confident that the software they are downloading from his company’s support site is legitimate. Which of the following tools or techniques should he utilize?
* Data validation
* Interrupt analyzer
* Digital certificate
* Pseudocode

Q65. A developer needs to apply a family of protocols to mediate network access. Authentication and Authorization has been implemented properly. Which of the following is the missing component?
* Management
* Accounting
* Auditing
* Inventory

Q66. An OT security practitioner wants to implement two-factor authentication (2FA). Which of the following is the least secure method to use for implementation?
* Out-of-band authentication (OOBA)
* 2FA over Short Message Service (SMS)
* Authenticator Apps for smartphones
* Fast Identity Online (FIDO) Universal 2nd Factor (U2F) USB key

Q67. Web forms that contain unvalidated fields are vulnerable to which of the following attacks? (Choose two.)
* Smurf
* Ping of death
* Cross-Site Scripting (XSS)
* Man-in-the-middle (MITM)
* SQL Injection (SQLi)

Q68. Which of the following encryption standards should an IoT developer select in order to implement an asymmetric key pair?
* Temporal Key Integrity Protocol (TKIP)
* Elliptic curve cryptography (ECC)
* Advanced Encryption Standard (AES)
* Triple Data Encryption Standard (3DES)

Q69. Requiring randomly generated tokens for each connection from an IoT device to the cloud can help mitigate which of the following types of attacks?
* Malformed URL injection
* Buffer overflow
* SSL certificate hijacking
* Session replay

Q70. Which of the following technologies allows for encryption of networking communications without requiring any configuration on IoT endpoints?
* Transport Layer Security (TLS)
* Internet Protocol Security (IPSec)
* Virtual private network (VPN)

* Elliptic curve cryptography (ECC)

Q71. You work for a business-to-consumer (B2C) IoT device company. Your organization wishes to publish an annual report showing statistics related to the volume and variety of sensor data it collects. Which of the following should your organization do prior to using this information?
* Confirm the devices they’ve sold are turned on
* Ensure all sensors are running the latest software
* Require customers to sign a subscription license
* Remove any customer-specific data

Q72. An IoT systems administrator needs to be able to detect packet injection attacks. Which of the follow methods or technologies is the administrator most likely to implement?
* Internet Protocol Security (IPSec) with Encapsulating Security Payload (ESP)
* Point-to-Point Tunneling Protocol (PPTP)
* Layer 2 Tunneling Protocol (L2TP)
* Internet Protocol Security (IPSec) with Authentication Headers (AH)

Q73. An IoT software developer wants the users of her software tools to know if they have been modified by someone other than her. Which of the following tools or techniques should she use?
* Encryption
* Obfuscation
* Hashing
* Fuzzing

Q74. An IoT security administrator wishes to mitigate the risk of falling victim to Distributed Denial of Service (DDoS) attacks. Which of the following mitigation strategies should the security administrator implement? (Choose two.)
* Block all inbound packets with an internal source IP address
* Block all inbound packets originating from service ports
* Enable unused Transmission Control Protocol (TCP) service ports in order to create a honeypot
* Block the use of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) through his perimeter firewall
* Require the use of X.509 digital certificates for all incoming requests

Q75. A DevOps engineer wants to provide secure network services to an IoT/cloud solution. Which of the following countermeasures should be implemented to mitigate network attacks that can render a network useless?
* Network firewall
* Denial of Service (DoS)/Distributed Denial of Service (DDoS) mitigation
* Web application firewall (WAF)
* Deep Packet Inspection (DPI)