# [Q22-Q43 Get 100% Passing Success With True ITS-110 Exam! [Dec-2023

[Q22-Q43] Get 100% Passing Success With True ITS-110 Exam! [Dec-2023]
Pause

**Get 100% Passing Success With True ITS-110 Exam! [Dec-2023 CertNexus ITS-110 PDF Questions - Exceptional Practice To Certified Internet of Things Security Practitioner**

CertNexus ITS-110 certification exam is an essential certification for professionals who work with IoT devices and networks. Certified Internet of Things Security Practitioner certification equips professionals with the skills and knowledge necessary to secure IoT devices and networks, and it is recognized globally. Certified Internet of Things Security Practitioner certification is vendor-neutral, making it an ideal certification for professionals who work with different IoT technologies and platforms.

**Q22.** Which of the following policies provides the BEST protection against identity theft when data stored on an IoT portal has been compromised?
* Data retention polices
* Data categorization policies
* Data anonymization policies
* Data disposal policies

**Q23.** 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

**Q24.** A compromised IoT device is initiating random connections to an attacker&#8217;s server in order to exfiltrate sensitive dat a. Which type of attack is being used?
* Man-in-the-middle (MITM)
* SSL session hijack
* Reverse shell
* Honeypot

**Q25.** An Agile Scrum Master working on IoT solutions needs to get software released for a new IoT product. Since bugs could be found after deployment, which of the following should be part of the overall solution?
* A money back guarantee, no questions asked
* Over-the-Air (OTA) software updates
* A lifetime transferable warranty
* Free firmware updates if the product is sent back to the manufacturer

**Q26.** Which of the following attacks relies on the trust that a website has for a user&#8217;s browser?
* Phishing
* SQL Injection (SQLi)
* Cross-Site Scripting (XSS)
* Cross-Site Request Forgery (CSRF)

**Q27.** You work for a multi-national IoT device vendor. Your European customers are complaining about their inability to access the personal information about them that you have collected. Which of the following regulations is your organization at risk of violating?
* Sarbanes-Oxley (SOX)
* General Data Protection Regulation (GDPR)
* Electronic Identification Authentication and Trust Services (elDAS)
* Database Service on Alternative Methods (DB-ALM)

**Q28.** Which of the following attacks utilizes Media Access Control (MAC) address spoofing?
* Network Address Translation (NAT)
* Man-in-the-middle (MITM)
* Network device fuzzing
* Unsecured network ports

**Q29.** Which of the following methods or technologies is most likely to be used in order to mitigate brute force attacks?
* Account lockout policy
* Automated security logging
* Role-based access control
* Secure password recovery

**Q30.** 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)

**Q31.** A hacker is able to eavesdrop on administrative sessions to remote IoT sensors. Which of the following has most likely been misconfigured or disabled?
* Secure Shell (SSH)
* Internet Protocol Security (IPSec)
* Telnet
* Virtual private network (VPN)

**Q32.** 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

**Q33.** Which of the following is one way to implement countermeasures on an IoT gateway to ensure physical security?
* Add tamper detection to the enclosure
* Limit physical access to ports when possible
* Allow quick administrator access for mitigation
* Implement features in software instead of hardware

**Q34.** An IoT developer wants to ensure all sensor to portal communications are as secure as possible and do not require any client-side configuration. Which of the following is the developer most likely to use?
* Virtual Private Networking (VPN)
* Public Key Infrastructure (PKI)
* IP Security (IPSec)
* Secure/Multipurpose Internet Mail Extensions (S/MIME)

**Q35.** Network filters based on Ethernet burned-in-addresses are vulnerable to which of the following attacks?
* Media Access Control (MAC) spoofing
* Buffer overflow
* Packet injection
* GPS spoofing

**Q36.** Accompany collects and stores sensitive data from thousands of IoT devices. The company&#8217;s IoT security administrator is concerned about attacks that compromise confidentiality. Which of the following attacks is the security administrator concerned about? (Choose two.)
* Salami
* Aggregation
* Data diddling
* Denial of Service (DoS)
* Inference

**Q37.** 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

**Q38.** If an attacker were able to gain access to a user&#8217;s machine on your network, which of the following actions would she most likely take next?
* Start log scrubbing
* Escalate privileges
* Perform port scanning
* Initiate reconnaissance

**Q39.** Recently, you purchased a smart watch from Company A. You receive a notification on your watch that you missed a call and have a new message. Upon checking the message, you hear the following:

&#8220;Hello, my name is Julie Simmons, and I&#8217;m with Company A. I want to thank you for your recent purchase and send you a small token of our appreciation. Please call me back at 888-555-1234. You will need to enter your credit card number, so we can authenticate you and ship your gift. Thanks for being a valued customer and enjoy your gift!&#8221; Which of the following types of attacks could this be?
* Phishing
* Spear phishing
* Whaling
* Vishing

**Q40.** 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

**Q41.** A manufacturer wants to ensure that user account information is isolated from physical attacks by storing credentials off-device. Which of the following methods or technologies best satisfies this requirement?
* Role-Based Access Control (RBAC)
* Password Authentication Protocol (PAP)
* Remote Authentication Dial-In User Service (RADIUS)
* Border Gateway Protocol (BGP)

**Q42.** A web application is connected to an IoT endpoint. A hacker wants to steal data from the connection between them. Which of the following is NOT a method of attack that could be used to facilitate stealing data?
* Cross-Site Request Forgery (CSRF)
* SQL Injection (SQLi)
* Cross-Site Scripting (XSS)
* LDAP Injection

**Q43.** A web administrator is concerned about injection attacks. Which of the following mitigation techniques should the web administrator implement?
* Configure single sign-on (SSO)
* Parameter validation
* Require strong passwords
* Require two-factor authentication (2FA)