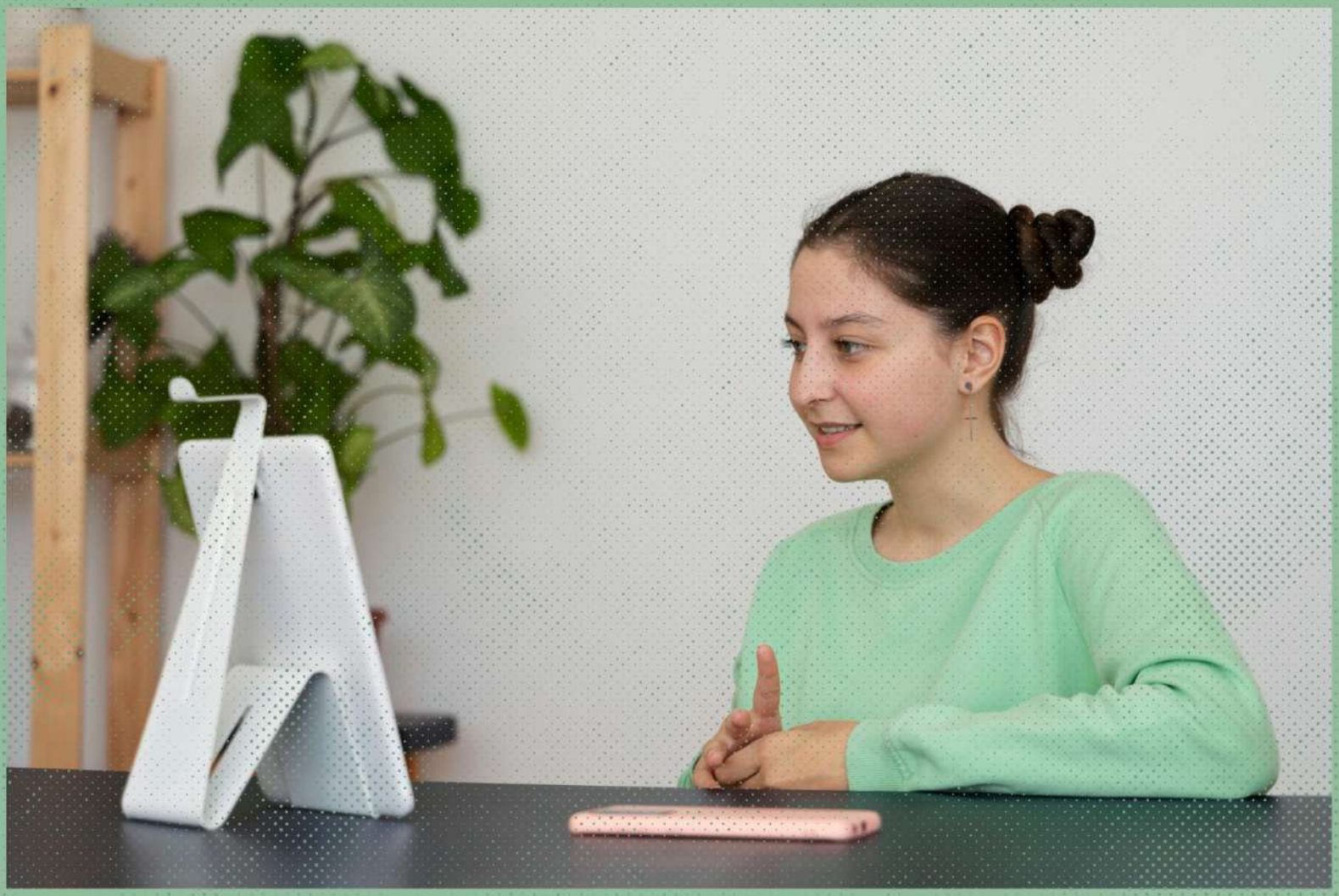
Certified Internet of Things Security Practitioner (CIoTSP)



Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

Securing IoT Portals

1.Identify common threats used to compromise unsecure web

- Account enumeration
- Weak default credentials
- Injection flaws
- Unsecure direct object references
- Sensitive data exposure
- CSRF
- Unvalidated redirects and forwards
- Session Management
- Malformed URLs
- Session replay
- Reverse shell
- Misconfiguration
- Weak account lockout settings
- No account lockout
- Unsecured credentials
- Lack of integration credentials on Edge devices

2.Implement countermeasures used to secure web, cloud

- Change default passwords
- Secure password recovery mechanisms
- Secure the web interface from XSS, SQLi, or CSRF
- Robust password policies
- Account lockout policies
- Protect against account enumeration
- 2FA if possible
- Granular role-based access

Implementing Authentication, Authorization, and Accounting

3.Identify common threats used to exploit weak authenticatn

- Lack of password complexity
- Poorly protected credentials
- Lack of 2FA
- Unsecure password recovery
- Privilege escalation
- Lack of RBAC
- Unsecure databases and datastores
- Lack of account lockout policy
- Lack of access auditing
- Lack of security monitoring
- Lack of security logging

4.countermeasures used to provide secure authentication

- Granular access control
- Password management
- Ensure re-authentication is required for sensitive features
- Event logging and IT/OT admin notification
- Security monitoring

Securing Network Services

5.Identify common threats used to exploit unsecure network .

- Vulnerable services
- Buffer overflow
- Open ports via UPnP
- Exploitable UDP services
- DoS/DDoS
- DoS via network device fuzzing
- Endpoint (address) spoofing
- Packet manipulation/injection
- Networking, protocols, radio communications

6 countermeasures used to provide secure network services.

- Port control
- Secure memory spaces
- DoS mitigation/DDoS
- Secure network nodes
- Secure field devices
- Secure network pathways

Securing Data

7.Identify common threats used to exploit unsecure data.

- Vulnerable data in motion
- Vulnerable data at rest
- Vulnerable data in use

8.Implement countermeasures used to secure data.

- Encrypt data in motion, at rest, and in use

Addressing Privacy Concerns

9.Identify common threats used to compromise privacy.

- Collection of unnecessary personal or sensitive information
- Unsecured data in transit or at rest
- Unauthorized access to personal information
- Lack of proper data anonymization
- Lack of data retention policies

10. Implement countermeasures used to ensure data privacy.

- Only collect critical data
- Protect sensitive data
- Comply with regulations/laws
- Authorize data users
- Data retention policies
- Data disposal policies
- End-user notification policies (GDPR)
- Enable courtesy notifications to end users
- Enable notifications as required by law

Securing Software/Firmware

11. Identify comn threats used to exploit unsecure software

- Poorly designed/tested software/firmware
- Unsecure updates/patches
- Firmware contains sensitive information
- Lack of OTA updates
- Constrained devices with non-existent security features
- Lack of end-to-end solution
- Software/firmware not digitally signed
- Unsecure bootloader/boot
- Unsecure key storage

12. countermeasures used to provd secure software/firmware.

- Digitally signed updates
- Remote update capability for, e.g., bootloader, firmware, OS
- Secure updates/digitally signed updates
- Root-of-trust/secure enclave
- Secure bootloader/boot, measured boot

Enhancing Physical Security

13. common threats used to exploit poor physical security.

- Access to software/configuration via physical ports
- Access to or removal of storage media
- Unprotected shell access for accessible ports
- Unrestricted physical access to vulnerable devices
- Easily disassembled devices

14. Implmt countermeasures used to ensure physical security.

- Protect data storage medium
- Encrypt data at rest
- Protect physical ports
- Tamper-resistant devices
- Limit physical access when possible
- Hardened security for shell access
- Limit administrative capabilities and access

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474