" LPI® Security Essentials (020-100)"

LPI Security Essentials - Course Introduction

This certificate covers a basic knowledge of IT security. The focus is the digital self-defense for an individual user. This includes a general understanding of the common security threats against individual computing systems, networks, services and identity as well as approaches to prevent and mitigate them.

021 Security Concepts

021.1 Goals, Roles and Actors (weight: 1)

Weight	1
Description	The candidate should understand the importance of IT security. This includes understanding of essential security goals as well as understanding various actors and roles in the field of IT security.

Key Knowledge Areas:

- Understanding of the importance of IT security
- Understanding of common security goals
- Understanding of common roles in security
- Understanding of common goals of attacks against IT systems and devices
- Understanding of the concept of attribution and related issues

Partial list of the used files, terms, and utilities:

- Confidentiality, integrity, availability, non-repudiation
- Hackers, crackers, script kiddies
- Black hat and white hat hackers
- Accessing, manipulating or deleting data
- Interrupting services, extorting ransom

- Industrial espionage

021.2 Risk Assessment and Management (weight: 2)

Weight	2
Description	The candidate should understand how to find and interpret relevant security information. This includes understanding the risk of a security vulnerability and determining the need and urgency for a reaction.

Key Knowledge Areas:

- Know common sources for security information
- Understanding of security incident classification schema and important types of security vulnerabilities
- Understanding of the concepts of security assessments and IT forensics
- Awareness of Information Security Management Systems (ISMS) and Information Security Incident Response Plans and Teams

Partial list of the used files, terms, and utilities:

- Common Vulnerabilities and Exposures (CVE)
- CVE ID
- Computer Emergency Response Team (CERT)
- Penetration testing
- Untargeted attacks and Advanced Persistent Threats (APT)
- Zero-day security vulnerabilities
- Remote execution and explication of security vulnerabilities
- Privilege escalation due to security vulnerabilities

021.3 Ethical Behavior (weight: 2)

Weight	2

Description	The candidate should understand the technical, financial, and legal implications of their behavior when using digital infrastructure. This includes understanding the potential harm caused by using security tools. Furthermore, the candidate should understand common concepts in copyright and privacy laws.

Key Knowledge Areas:

- Understanding the implications for others of actions taken related to security
- Handling information about security vulnerabilities responsibly
- Handling confidential information responsibly
- Awareness of personal, financial, ecological, and social implication of errors and outages in information technology services
- Awareness of legal implications of security scans, assessments, and attacks

Partial list of the used files, terms, and utilities:

- Responsible Disclosure and Full Disclosure
- Bug Bounty programs
- Public and private law
- Penal law, privacy law, copyright law
- Liability, financial compensation claims

022 Encryption

022.1 Cryptography and Public Key Infrastructure (weight: 3)

Weight	3
Description	The candidate should understand the concepts of symmetric and asymmetric encryption as well as other types of commonly used cryptographic algorithms. Furthermore, the candidate should understand how digital certificates are used to associate cryptographic keys with individual persons and organizations.

Key Knowledge Areas:

- Understanding of the concepts of symmetric, asymmetric, and hybrid cryptography

- Understanding of the concept of Perfect Forward Secrecy
- Understanding of the concepts of hash functions, ciphers, and key exchange algorithms
- Understanding of the differences between end-to-end encryption and transport encryption
- Understanding of the concepts of Public Key Infrastructures (PKI), Certificate Authorities, and Trusted Root-CAs
- Understanding of the concepts X.509 certificates
- Understanding of how X.509 certificates are requested and issued
- Awareness of certificate revocation
- Awareness of Let’s Encrypt
- Awareness of important cryptographic algorithms

Partial list of the used files, terms, and utilities:

- Public Key Infrastructures (PKI)
- Certificate Authorities
- Trusted Root-CAs
- Certificate Signing Requests (CSR) and certificates
- X.509 certificate fields: Subject, Issuer, Validity
- RSA, AES, MD5, SHA-256, Diffie–Hellman key exchange, Elliptic Curve Cryptography

022.2 Web Encryption (weight: 2)

Weight	2
Description	The candidate should understand the concepts of HTTPS. This includes verifying the identity of web servers and understanding common browser error messages related to security.

Key Knowledge Areas:

- Understanding of the major differences between plain text protocols and transport encryption

- Understanding of the concepts of HTTPS
- Understanding of important fields in X.509 certificates for the use with HTTPS
- Understanding of how X.509 certificates are associated with a specific web site
- Understanding of the validity checks web browsers perform on X.509 certificates
- Determining whether or not a website is encrypted, including common browser messages

Partial list of the used files, terms, and utilities:

- HTTPS, TLS, SSL
- X.509 certificate fields: subject, Validity, subjectAltName

022.3 Email Encryption (weight: 2)

Weight	2
Description	The candidate should understand the concepts of OpenPGP and S/MIME for email encryption. This includes handling OpenPGP keys and S/MIME certificates as well as sending and receiving encrypted emails.

Key Knowledge Areas:

- Understanding of email encryption and email signatures
- Understanding of OpenPGP
- Understanding of S/MIME
- Understanding of the role of OpenPGP key servers
- Understanding of the role of certificates for S/MIME
- Understanding of how PGP keys and S/MIME certificates are associated with an email address
- Using Mozilla Thunderbird to send and receive encrypted email using OpenPGP and S/MIME

Partial list of the used files, terms, and utilities:

- GnuPGP, GPG keys, key servers

- S/MIME and S/MIME certificates

022.4 Data Storage Encryption (weight: 2)

Weight	2
Description	The candidate should understand the concepts of file encryption and storage device encryption. Furthermore, the candidate should be able to encrypt data stored on local storage devices and in the cloud.

Key Knowledge Areas:

- Understanding of the concepts of data, file, and storage device encryption
- Using VeraCrypt to store data in an encrypted container or an encrypted storage devices
- Understanding the core features of BitLocker
- Using Cryptomator to encrypt files stored in file storage cloud services

Partial list of used files, terms, and utilities:

- VeraCrypt
- BitLocker
- Cryptomator

023 Device and Storage Security

023.1 Hardware Security (weight: 2)

Weight	2
Description	The candidate should understand security aspects of hardware. This includes understanding the various types of computer devices as well as their major components. Furthermore, the candidate should understand the security implications of various devices that interact with a computer as well as the security implications of physical access to a device.

Key Knowledge Areas:

- Understanding of the major components of a computer

- Understanding of the smart devices and the Internet of Things (IoT)
- Understanding of the security implications of physical access to a computer
- Understanding of USB devices devices types, connections, and security aspects
- Understanding of Bluetooth devices types, connections, and security aspects
- Understanding of RFID devices types, connections, and security aspects
- Awareness of Trusted Computing

Partial list of used files, terms, and utilities:

- Processors, memory, storage, network adapters
- Tablets, smartphones, smart tvs, routers, printers smart home, alarm, IoT devices (e.g. light bulbs, thermostats, TVs)
- USB
- Bluetooth
- RFID

023.2 Application Security (weight: 2)

Weight	2
Description	The candidate should understand the security aspects of software. This includes securely installing software, managing software updates, and protecting software from unintended network connections.

Key Knowledge Areas:

- Understanding of common types of software
- Understanding of various sources for applications and ways to securely procure and install software
- Understanding of updates for firmware, operating systems, and applications
- Understanding of sources for mobile applications
- Understanding of common security vulnerabilities in software

- Understanding of the concepts of local protective software

Partial list of used files, terms, and utilities:

- Firmware, operating systems, applications
- App stores
- Local packet filters, endpoint firewalls, application layer firewalls
- Buffer overflows, SQL injections

023.3 Malware (weight: 3)

Weight	3
Description	The candidate should understand the various types of malware. This includes understanding of how they are installed on a device, what effects they cause, and how to protect against malware.

Key Knowledge Areas:

- Understanding of common types of malware
- Understanding of the concepts of rootkit and remote access
- Understanding of virus and malware scanners
- Awareness of the risk of malware used for spying, data exfiltration, and address books copies

Partial list of used files, terms, and utilities:

- Viruses, ransomware, trojan malware, adware, cryptominers
- Backdoors and remote access
- File copying, keylogging, camera, microphone hijacking

023.4 Data Availability (weight: 2)

Weight	2

Description	The candidate should understand how to ensure the availability of their data. This includes storing data on appropriate devices and services as well as creating backups.

Key Knowledge Areas:

- Understanding of the importance of backups
- Understanding of common backup types and strategies
- Understanding of the security implications of backups
- Creating and securely storing backups
- Understanding of data storage, access, and sharing in cloud services
- Understanding of the security implications of cloud storage and shared access in the cloud
- Awareness of the dependence on Internet connection and the synchronization of data between cloud services and local storage

Partial list of used files, terms, and utilities

- Full, differential and incremental backups
- Backup retention
- File sharing cloud services

024 Network and Service Security

024.1 Networks, Network Services and the Internet (weight: 4)

Weight	4
Description	The candidate should understand the concepts of computer networks and the Internet. This includes basic knowledge of various network media types, addressing, routing, and packet forwarding as well as understanding of the most important protocols used in the Internet.

Key Knowledge Areas:

- Understanding of the various types of network media and network devices

- Understanding of the concepts of IP networks and the Internet
- Understanding of the concepts of routing and Internet Service Providers (ISPs)
- Understanding of the concepts of MAC and link-layer addresses, IP addresses, TCP and UDP ports, and DNS
- Understanding of the concepts of cloud computing

Partial list of used files, terms, and utilities:

- Wired networks, WiFi networks, cellular networks
- Switches, Routers, Access Points
- Default Router
- Internet Service Provider
- IPv4, IPv6
- TCP, UDP, ICMP, DHCP
- DNS, DNS host names, forward DNS, reverse DNS
- Cloud computing
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

024.2 Network and Internet Security (weight: 3)

Weight	3
Description	The candidate should understand common security aspects of using networks and the Internet. This includes understanding of common security threats against networks and networked computers, approaches for mitigation, as well as the ability to securely connect to a wired or wireless network.

Key Knowledge Areas:

- Understanding of the implications of link layer access

- Understanding of the risks and secure use of WiFi networks
- Understanding of the concepts of traffic interception
- Understanding of common security threats in the Internet along with approaches of mitigation

Partial list of the used files, terms, and utilities:

- Link layer
- Unencrypted and public WiFi
- WiFi security and encryption
- WEP, WPA, WPA2
- Traffic interception
- Man in the Middle attacks
- DoS and DDoS attacks
- Botnets
- Packet filters

024.3 Network Encryption and Anonymity (weight: 3)

Weight	3
Description	The candidate should understand the concepts of virtual private networks (VPN). This includes using a VPN provider to encrypt transmitted data. Candidates should understand recognition and anonymity concepts when using the Internet as well as anonymization tools, such as TOR.

Key Knowledge Areas:

- Understanding of virtual private networks (VPN)
- Understanding of the concepts of end-to-end encryption
- Understanding anonymity and recognition in the Internet
- Identification due to link layer addresses and IP addresses

- Understanding of the concepts of proxy servers
- Understanding of the concepts of TOR
- Awareness of the Darknet
- Awareness of cryptocurrencies and their anonymity aspects

Partial list of used files, terms, and utilities:

- Virtual Private Network (VPN)
- Public VPN providers
- Organization-specific VPN (e.g. company or university VPNs)
- End-to-end encryption
- Transfer encryption
- Anonymity
- Proxy servers
- TOR
- Hidden service
- .onion
- Blockchain

025 Identity and Privacy

025.1 Identity and Authentication (weight: 3)

Weight	3
Description	The candidate should understand common concepts on how to prove their identity when using online services. This includes using a password manager, multi-factor authentication, and single sign-on, as well as being aware of common security threats regarding individual identities.

Key Knowledge Areas:

- Understanding of the concepts of digital identities.

- Understanding of the concepts of authentication, authorization, and accounting
- Understanding of the characteristics of secure password (e.g. length, special characters, change frequencies, complexity)
- Using a password manager
- Understanding of the concepts of security questions and account recovery tools
- Understanding of the concepts of multi-factor authentication (MFA), including common factors
- Understanding of the concepts of single sign-on (SSO) and social media logins
- Understanding of the role of email accounts for IT security
- Understanding of how passwords are stored in online services
- Understanding of common attacks against passwords
- Monitoring personal accounts for password leaks (e.g. search engine alerts for usernames and password leak checkers)
- Understanding of the security aspects of online banking and credit cards

Partial list of used files, terms, and utilities:

- Online and offline password managers
- keepass2
- Single sign-on (SSO)
- Two-factor authentication (2FA) and multi-factor authentication (MFA)
- One-time passwords (OTP), time-based one-time passwords (TOTP)
- Authenticator applications
- Password hashing and salting
- Brute force attacks, directory attacks, rainbow table attacks

025.2 Information Confidentiality and Secure Communication (weight: 2)

Weight	2
Description	The candidate should understand how to keep confidential information secret and ensure the confidentiality of digital communication. This includes recognizing attempts of phishing and social engineering, as well as using secure means of communication.

Key Knowledge Areas:

- Understanding the implications and risks of data leaks and intercepted communication
- Understanding of phishing and social engineering and scamming
- Understanding the concepts of email spam filters
- Securely handling of received email attachments
- Sharing information securely and responsibly using email cloud shares and messaging services
- Using encrypted instant messaging

Partial list of the used files, terms, and utilities:

- Phishing and social engineering
- Identity theft
- Scamming and scareware
- Email spam, email spam filtering
- Non-disclosure agreements (NDA)
- Information classification

025.3 Privacy Protection (weight: 2)

Weight	2
Description	The candidate should understand the importance of the confidentiality of personal information. This includes managing privacy settings in various online services and social media as well as being aware of common security threats regarding personal information.

Key Knowledge Areas:

- Understanding of the importance of personal information
- Understanding of how personal information can be used for a malicious purpose
- Understanding of the concepts of information gathering, profiling, and user tracking
- Managing profile privacy settings on social media platforms and online services
- Understanding of the risk of publishing personal information
- Understanding of the rights regarding personal information (e.g. GDPR)

Partial list of the used files, terms, and utilities:

- Stalking and cybermobbing
- HTTP cookies, browser fingerprinting, user tracking
- Script blockers and ad blockers in web browsers
- Profiles in online services and social media
- Contacts and privacy settings in social media