EUROPEAN INFORMATION TECHNOLOGIES CERTIFICATION INSTITUTE, ASBL.

Brussels, Belgium, European Union

CERTIFICATE

Michal Klos

Has successfully completed test requirements of
The European Information Technologies Certification Programme

EITC/IS/OS Operating systems security

Certification Programme examination result: 65%

Certification Programme description:

Introduction to operating systems: classification of operating systems (based on methods of processing, number of executed commands or number of users, other types of operating systems), principles of functioning of operating systems (instruction execution cycle, interrupts, memory protection, clock interruption); processes, resources, threads: process and resource handling (types of system core compilation in process and resource management, managers, cycle of states and processes changes, resource classification, process queues, context switching, basic operations on processes and resources), threads (thread implementation, thread context switching, basic operations on threads), thread and process implementation in Linux and Windows; file system - logical layer: files in operating system (operating system's tasks, file attributes, file types, file structure, methods of file access, basic operations on files), file access interface in unix-like systems, logical organization of file system (zones, operations on catalogs, catalog logical structure); file system - physical layer: disk space assignment (continuous assignment, list assignment, chain assignment, index assignment), free space management, catalog implementation, cache storage in file system, file system integrity, file access synchronization; file system - overview of implementations (CP/M, MS DOS and Windows 9x [FAT12/16/32], ISO 9660, UNIX, NTFS); importance of security, security threats, general problems of security, security strategy, security policies, security management paradigms and norms; basic problems of operating systems' security: introduction, security breaches, determining the operating system of attacked computer, authentication, resource access rights (standards: POSIX 1003.1, POSIX 1003.1e/1003.2c, access lists - ACL), special permissions in Unix, malware (viruses and bugs), masked communication channels; authentication and access control: general principles of authentication in Linux, file access rights in Unix-like systems, POSIX ACL mechanism in Windows and Linux (local access control in Linux and MS Windows), modular authentication and access control systems - RAM mechanism; permissions' limitation and delegation, trust domains, remote access control: controlled application execution environment, controlled layers of server operating systems, permissions delegation (limits mechanism, SUDO mechanism, SUID and SGID mechanisms), mechanisms of remote access control (usage of trust domains, rlogin command in Linux, securing network services with tcpd); operating system security amplification in MS Windows network environments: user accounts, file system, data encryption (encryption on file system level, data archives with cryptographical protection, e-mail cryptographical protection), network environment (network neighbourhood and network shares, hiding the computer in network, network connections, network firewalls)

Certificate Programme version/revision: EITC/IS/OSv1r2

CERTIFICATE ID: **EITC/IS/OS/LEH/18004658**

To validate authenticity of this certificate or review its programme and test results scan/click QR code or visit:
www.eitci.org/validate

DATE OF ISSUE:
October 2018
Brussels, Belgium
European Union