UNIX/Linux – Security, Secure Communication and Cryptography

Course code: UNIXB2

This course is designed for network server administrators who need secure both data on the server server and the communication with the server. The participants will familiarize themselves with the basics of encryption in the computer security field. They will also learn to work with PGP (GnuPG), SSL, DM-Crypt systems, etc.

Who is the course for

The course is designed for network administrators and network server administrators who use OS UNIX and who would

like to learn to make the communication of these servers with their surroundings secure.

What we teach you

The participants will learn basic principles of cryptography and encryption in the computer security field. They will also

learn how to implement PGP (GnuPG), SSL systems, etc.

Required skills

Good knowledge of OS UNIX

Teaching materials

GOPAS study materials

Course outline

 Basic principles, methods and applications of cryptography

Overview and the use of common cryptographic algorithms - HASH function, symmetric/conventional and asymmetric methods
HASH function, overview of characteristics and the use (MDx, SHAx, etc.)
Symmetric methods, overview of characteristics and the principle of running of these algorithms (DES, 3DES,AES, etc.)
Asymmetric methods, overview of characteristics and the principle of running of these algorithms, application (DH, RSA, DSA,etc.)
Some chosen applications, digital signature, confidential relations - certificates, etc.

Practical applications of cryptography

PGP (GnuPG) system, application

SSL/TLS system, implementation of OpenSSL

Work with keys and certificates

Stunnel programme

Encrypted disks using CryptoLoop and DMCrypt

GOPAS®