UNIX/Linux – bezpečnost dat, bezpečná komunikace, šifrování

Kód kurzu: UNIXB2

Kurz je určen pro správce síťových serverů, kteří potřebují zabezpečit jak data na serveru server, tak komunikaci se serverem. Účastnící se seznámí se základy šifrování v oblasti počítačové bezpečnosti. Dále se naučí prakticky používat systémy PGP (GnuPG), SSL/TLS, DM-Crypt, atd.

Pro koho je kurz určen

Kurz je určen pro správce sítí a síťových serverů s OS UNIX, kteří se chtějí naučit zabezpečit komunikaci těchto serverů se svým okolím.

Co Vás naučíme

Účastníci kurzu se naučí základním principům kryptologie a šifrování v prostředí počítačové bezpečnosti. Dále se naučí prakticky implementovat systémy PGP (GnuPG), SSL, atd.

Požadované vstupní znalosti

Dobrá znalost OS UNIX.

Studijní materiály

Studijní materiál GOPAS, a.s.

Osnova kurzu

Základní principy, metody a aplikace kryptologie

- Přehled a užití běžných kryptologických algoritmů - HASH funkce, symetrické/konvenční a asymetrické metody
- HASH funkce, přehled vlastností a použití (MDx, SHAx, atd.)
- Symetrické metody, přehled vlastností a princip fungování těchto algoritmů, použití (DES, 3DES,AES, atd.)
- Asymetrické metody, přehled vlastností a princip fungování těchto algoritmů, použití (DH, RSA, DSA, atd.)
- Některé vybrané aplikace, digitální podpis, vztahy důvěry - certifikáty, atd.

Praktické aplikace kryptologie

- Systém PGP (GnuPG), použití
- Systém SSL/TLS, imlementace OpenSSL
- Práce s klíči a certifikáty
- Program Stunnel
- Šifrované disky pomocí CryptoLoop a DMCrypt

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk